internetsecuritysuite

Guida dell'utente

Versione 8.0

McAfee®

COPYRIGHT

Copyright © 2005 McAfee, Inc. Tutti i diritti riservati. È vietato riprodurre, trasmettere, trascrivere, archiviare in un sistema di recupero dei dati o tradurre in altra lingua completamente o in parte questo documento con qualsiasi mezzo senza previa autorizzazione scritta di McAfee, Inc., o di un suo fornitore o di una sua consociata.

ATTRIBUZIONI DEI MARCHI DI FABBRICA

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (E IN KATAKANA), ACTIVESHIELD, ANTIVIRUS ANYWARE E DESIGN, CLEAN-UP, DESIGN (E STILIZZATA), DESIGN (N STILIZZATA), ENTERCEPT, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (E IN KATAKANA), EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (E IN KATAKANA), GUARD DOG, HOMEGUARD, HUNTER, INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, M E DESIGN, MCAFEE, MCAFEE (E IN KATAKANA), MCAFEE E DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS, NET TOOLS (E IN KATAKANA), NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (E IN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (E IN KATAKANA), WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, YOUR E-BUSINESS DEFENDER, YOUR NETWORK. OUR BUSINESS. sono marchi o marchi registrati di McAfee, Inc. e/o delle rispettive consociate negli Stati Uniti e/o in altri paesi. Il rosso utilizzato con riferimento alla protezione è una caratteristica distintiva dei prodotti con marchio McAfee. Tutti i marchi registrati e non registrati citati nel presente documento sono di proprietà esclusiva dei rispettivi titolari.

INFORMAZIONI SULLA LICENZA

Contratto di licenza

AVVISO AGLI UTENTI: LEGGERE ATTENTAMENTE IL TESTO DEL CONTRATTO RELATIVO ALLA LICENZA ACQUISTATA, CHE STABILISCE LE CONDIZIONI GENERALI DI FORNITURA PER L'UTILIZZO DEL SOFTWARE CONCESSO IN LICENZA. NEL CASO IN CUI NON SI SAPPIA CON ESATTEZZA CHE TIPO DI LICENZA È STATA ACQUISTATA, CONSULTARE I DOCUMENTI DI VENDITA E ALTRE AUTORIZZAZIONI CONNESSE O LA DOCUMENTAZIONE RELATIVA ALL'ORDINE DI ACQUISTO CHE ACCOMPAGNA LA CONFEZIONE DEL SOFTWARE O CHE È STATA RICEVUTA SEPARATAMENTE IN RELAZIONE ALL'ACQUISTO MEDESIMO (SOTTO FORMA DI OPUSCOLO, FILE CONTENUTO NEL CD DEL PRODOTTO O FILE DISPONIBILE SUL SITO WEB DAL QUALE È STATO ESEGUITO IL DOWNLOAD DEL SOFTWARE). SE NON SI ACCETTANO ALCUNI O TUTTI I TERMINI DEL CONTRATTO, ASTENERSI DALL'INSTALLARE IL SOFTWARE. SE PREVISTO DAL CONTRATTO, L'UTENTE POTRÀ RESTITUIRE IL PRODOTTO A MCAFEE O AL PUNTO VENDITA IN CUI È STATO ACQUISTATO ED ESSERE INTERAMENTE RIMBORSATO.

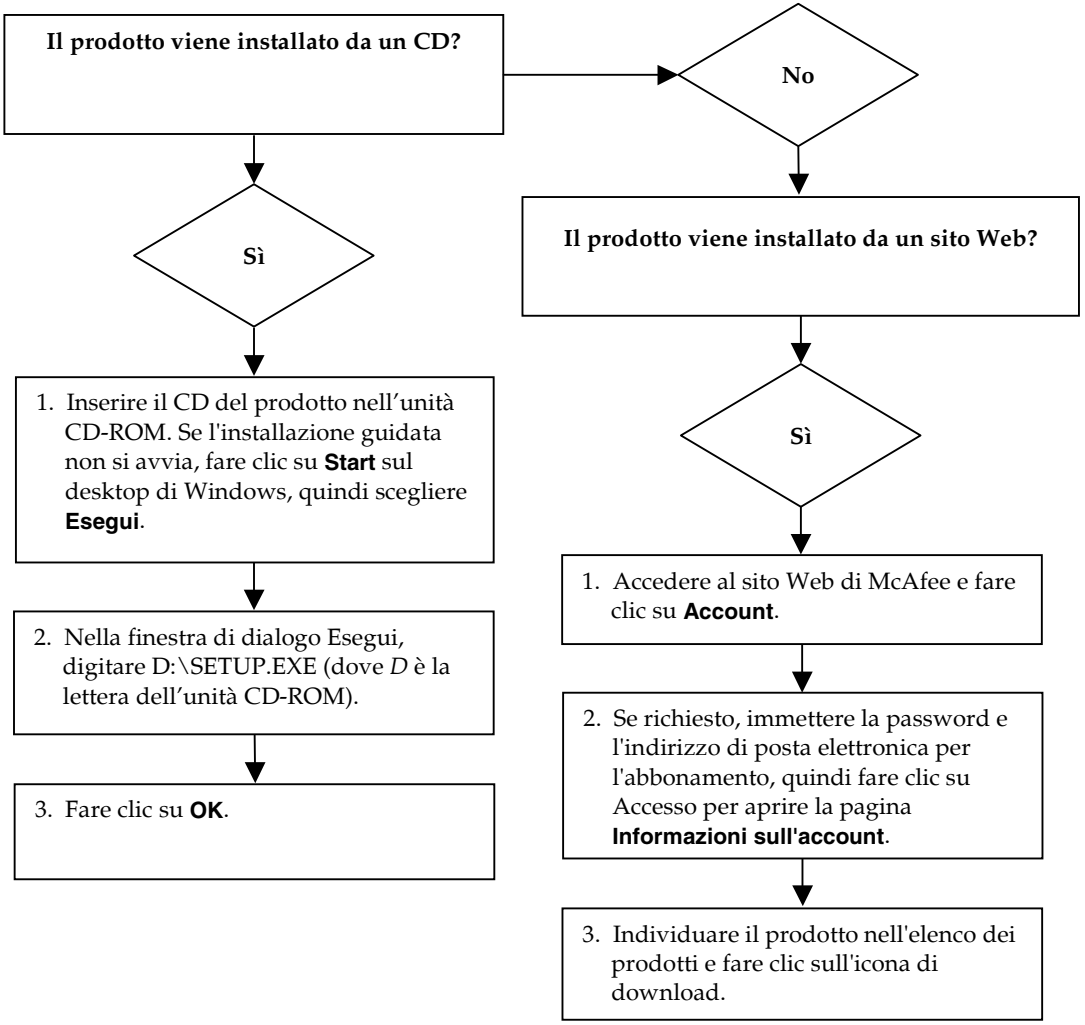
Attribuzioni

Questo prodotto include o potrebbe includere:

♦ Software sviluppato da OpenSSL Project per l'utilizzo nell'OpenSSL Toolkit (http://www.openssl.org/). ♦ Software crittografico scritto da Eric A. Young e software scritto da Tim J. Hudson. ♦ Software concesso in licenza o in sublicenza all'utente in base a licenze GNU GPL (General Public License) o a licenze Free Software analoghe che autorizzano l'utente, tra l'altro, a copiare, modificare e ridistribuire alcuni programmi o parte di essi e ad accedere al codice sorgente. La convenzione GPL prevede che, per qualsiasi software coperto da licenza GPL e distribuito ad altri utenti in formato binario eseguibile, debba essere reso disponibile anche il relativo codice sorgente. Per qualsiasi software coperto da licenza GPL, è reso disponibile sul presente CD il relativo codice sorgente. Qualora, in base a licenze Free Software, i diritti di utilizzo, copia o modifica di un programma che McAfee è tenuta a concedere siano più ampi dei diritti concessi in base al presente contratto, i suddetti diritti avranno la precedenza sui diritti e le restrizioni qui previste. ♦ Software originariamente scritto da Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. ♦ Software originariamente scritto da Robert Nordier, Copyright © 1996-7 Robert Nordier. ♦ Software scritto da Douglas W. Sauder. ♦ Software sviluppato da Apache Software Foundation (http://www.apache.org/). Per ottenere una copia del contratto di licenza di questo software, visitare il sito www.apache.org/licenses/LICENSE-2.0.txt. ♦ International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation e altri. ♦ Software sviluppato da CrystalClear Software, Inc., Copyright © 2000 CrystalClear Software, Inc. ♦FEAD® tecnologia Optimizer®, Copyright Netopsystems AG, Berlino, Germania. ♦ Outside In® Viewer Technology © 1992-2001 Stellent Chicago, Inc. e/o Outside In® HTML Export, © 2001 Stellent Chicago, Inc. ♦ Software protetto da copyright di Thai Open Source Software Center Ltd. e Clark Cooper, © 1998, 1999, 2000. ♦ Software protetto da copyright dei manutentori di software Expat. ♦ Software protetto da copyright di The Regents of the University of California, © 1989. ♦ Software protetto da copyright di Gunnar Ritter. ♦ Software protetto da copyright di Sun Microsystems®, Inc.© 2003. ♦ Software protetto da copyright di Gisle Aas. © 1995-2003. ♦ Software protetto da copyright di Michael A. Chase, © 1999-2000. ♦ Software protetto da copyright di Neil Winton, © 1995-1996. ♦ Software protetto da copyright di RSA Data Security, Inc., © 1990-1992. ♦ Software protetto da copyright di Sean M. Burke, © 1999, 2000. ♦ Software protetto da copyright di Martijn Koster, © 1995. ♦ Software protetto da copyright di Brad Appleton, © 1996-1999. ♦ Software protetto da copyright di Michael G. Schwern, © 2001. ♦ Software protetto da copyright di Graham Barr, © 1998. ♦ Software protetto da copyright di Larry Wall e Clark Cooper, © 1998-2000. ♦ Software protetto da copyright di Frodo Looijaard, © 1997. ♦ Software protetto da copyright di Python Software Foundation, Copyright © 2001, 2002, 2003. Per ottenere una copia del contratto di licenza di questo software, visitare il sito www.python.org. ♦ Software protetto da copyright di Beman Dawes, © 1994-1999, 2002. ♦ Software scritto da Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. ♦ Software protetto da copyright di Simone Bordet & Marco Cravero, © 2002. ♦ Software protetto da copyright di Stephen Purcell, © 2001. ♦ Software sviluppato dall'Indiana University Extreme! Lab (http://www.extreme.indiana.edu/). ♦ Software protetto da copyright di International Business Machines Corporation e altri, © 1995-2003. ♦ Software sviluppato da University of California, Berkeley e suoi contributori. ♦ Software sviluppato da Ralf S. Engelschall <rse@engelschall.com> per l'utilizzo nel mod_ssl project (http://www.modssl.org/). ♦ Software protetto da copyright di Kevlin Henney, © 2000-2002. ♦ Software protetto da copyright di Peter Dimov e Multi Media Ltd. © 2001, 2002. ♦ Software protetto da copyright di David Abrahams, © 2001, 2002. Per la documentazione, vedere http://www.boost.org/libs/bind/bind.html. ♦ Software protetto da copyright di Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. ♦ Software protetto da copyright di Boost.org, © 1999-2002. ♦ Software protetto da copyright di Nicolai M. Josuttis, © 1999. ♦ Software protetto da copyright di Jeremy Siek, © 1999-2001. ♦ Software protetto da copyright di Daryle Walker, © 2001. ♦ Software protetto da copyright di Chuck Allison e Jeremy Siek, © 2001, 2002. ♦ Software protetto da copyright di Samuel Krempp, © 2001. Per aggiornamenti, documentazione e riepilogo delle revisioni, vedere http://www.boost.org. ♦ Software protetto da copyright di Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. ♦ Software protetto da copyright di Cadenza New Zealand Ltd., © 2000. ♦ Software protetto da copyright di Jens Maurer, © 2000, 2001. ♦ Software protetto da copyright di Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000. ♦ Software protetto da copyright di Ronald Garcia, © 2002. ♦ Software protetto da copyright di David Abrahams, Jeremy Siek e Daryle Walker, © 1999-2001. ♦ Software protetto da copyright di Stephen Cleary (shammah@voyager.net), © 2000. ♦ Software protetto da copyright di Housemarque Oy <http://www.housemarque.com>, © 2001. ♦ Software protetto da copyright di Paul Moore, © 1999. ♦ Software protetto da copyright di Dr. John Maddock, © 1998-2002. ♦ Software protetto da copyright di Greg Colvin e Beman Dawes, © 1998, 1999. ♦ Software protetto da copyright di Peter Dimov, © 2001, 2002. ♦ Software protetto da copyright di Jeremy Siek e John R. Bandela, © 2001. ♦ Software protetto da copyright di Joerg Walter e Mathias Koch, © 2000-2002.

Scheda di avvio rapido

Se si installa il prodotto da un CD o da un sito Web, stampare questa pratica pagina di riferimento.


Il prodotto viene installato da un CD?
No
Sì
Il prodotto viene installato da un sito Web?
Sì
1. Inserire il CD del prodotto nell'unità CD-ROM. Se l'installazione guidata non si avvia, fare clic su **Start** sul desktop di Windows, quindi scegliere **Esegui**.
2. Nella finestra di dialogo Esegui, digitare D:\SETUP.EXE (dove *D* è la lettera dell'unità CD-ROM).
3. Fare clic su **OK**.
1. Accedere al sito Web di McAfee e fare clic su **Account**.
2. Se richiesto, immettere la password e l'indirizzo di posta elettronica per l'abbonamento, quindi fare clic su Accesso per aprire la pagina **Informazioni sull'account**.
3. Individuare il prodotto nell'elenco dei prodotti e fare clic sull'icona di download.

McAfee si riserva il diritto di modificare i Piani di aggiornamento e assistenza e i criteri in qualsiasi momento senza preavviso. McAfee e i relativi nomi di prodotti sono marchi o marchi registrati di McAfee, Inc. e/o delle relative società affiliate negli USA e/o in altri paesi.
© 2005 McAfee, Inc. Tutti i diritti riservati.

Per ulteriori informazioni

Per visualizzare le Guide dell'utente sul CD del prodotto, controllare che Acrobat Reader sia installato; in caso contrario, installarlo dal CD del prodotto McAfee.

1. Inserire il CD del prodotto nell'unità CD-ROM.
2. Aprire Esplora risorse. Fare clic su **Start** sul desktop di Windows, quindi su **Cerca**.
3. Individuare la cartella Manuali e fare doppio clic sul file .PDF della Guida dell'utente che si desidera aprire.

Vantaggi della registrazione

Per inviare la registrazione direttamente a McAfee, si consiglia di attenersi alla facile procedura contenuta nel prodotto acquistato. Oltre a garantire assistenza tecnica puntuale e competente, la registrazione offre i seguenti vantaggi:

- Supporto elettronico GRATUITO
- Aggiornamenti dei file di definizione dei virus (.DAT) per un anno dall'installazione quando si acquista il software VirusScan

  Per informazioni sui prezzi di un ulteriore anno di abbonamento per gli aggiornamenti delle definizioni dei virus, visitare il sito http://www.mcafee.com/.
- 60 giorni di garanzia per l'eventuale sostituzione del CD del software nel caso in cui sia difettoso o danneggiato
- Aggiornamenti dei filtri di SpamKiller per un anno dall'installazione quando si acquista il software SpamKiller

  Per informazioni sui prezzi di un ulteriore anno di abbonamento per gli aggiornamenti dei filtri, visitare il sito http://www.mcafee.com/.
- Aggiornamenti del pacchetto McAfee Internet Security per un anno dall'installazione quando si acquista il software MIS

  Per informazioni sui prezzi di un ulteriore anno di abbonamento per gli aggiornamenti dei contenuti, visitare il sito http://www.mcafee.com.

Supporto tecnico

Per il supporto tecnico, visitare il sito

http://www.mcafeehelp.com/.

Il sito dell'assistenza consente di accedere 24 ore su 24 alla semplice procedura di risposta guidata alle domande più comuni.

Gli utenti più esperti possono anche provare le opzioni avanzate, tra cui una ricerca basata su parole chiave e un sistema di Guida in linea. Se non si trova una soluzione, si può inoltre accedere alle opzioni GRATUITE Chat Now! ed E-mail Express. Le opzioni di chat e di posta elettronica consentono di entrare rapidamente in contatto tramite Internet con i tecnici qualificati del servizio di supporto, senza costi aggiuntivi. In alternativa, le informazioni sull'assistenza telefonica sono reperibili presso il sito

http://www.mcafeehelp.com/.

Sommario

Scheda di avvio rapido iii

1 Introduzione 11

Software McAfee Internet Security 12
Requisiti di sistema 12
Utilizzo di McAfee SecurityCenter 13
Rimozione dei programmi di Internet Security Suite 14

2 McAfee VirusScan 15

Nuove funzioni 15
Verifica di VirusScan 17
- Verifica di ActiveShield 17
- Verifica della funzione Scansione 17

Utilizzo di ActiveShield 19
- Attivazione o disattivazione di ActiveShield 19
- Configurazione delle opzioni di ActiveShield 20
- Informazioni suli avvisi di protezione 29

Scansione manuale del computer 33
- Ricerca manuale di virus e altre minacce 33
- Ricerca automatica di virus e altre minacce 37
- Informazioni sul rilevamento delle minacce 39

Gestione dei file in quarantena 40
Creazione di un disco di ripristino 42
- Protezione da scrittura di un disco di ripristino 43
- Utilizzo di un disco di ripristino 44
- Aggiornamento di un disco di ripristino 44

Segnalazione automatica dei virus 44
- Segnalazione per la World Virus Map 44
- Visualizzazione della World Virus Map 46

Aggiornamento di VirusScan 47
- Verifica automatica degli aggiornamenti 47
- Verifica manuale degli aggiornamenti 47

3 McAfee Personal Firewall Plus 49

Nuove funzioni 49
Rimozione di altri firewall 51
Impostazione del firewall predefinito 51
Impostazione del livello di protezione 52
Verifica di McAfee® Personal Firewall Plus 54
Informazioni sulla pagina Riepilogo 54
Informazioni sulla pagina Applicazioni Internet 59
Modifica delle regole delle applicazioni 60
Autorizzazione e blocco delle applicazioni Internet 61
Informazioni sulla pagina Eventi in ingresso 61
Informazioni sugli eventi 62
Visualizzazione degli eventi nel registro Eventi in ingresso 64
Risposta agli eventi in ingresso 66
Gestione del registro Eventi in ingresso 70
Informazioni sugli avvisi 72
Avvisi rossi 72
Avvisi verdi 78
Avvisi blu 79

4 McAfee Privacy Service 81

Funzioni 81
L'amministratore 81
Assistente di installazione 82
Recupero della password di amministratore 82
L'utente di avvio 83
Apertura di McAfee Privacy Service 83
Apertura e accesso a Privacy Service 83
Disattivazione di Privacy Service 83
Aggiornamento di McAfee Privacy Service 84
Aggiunta di utenti 84
Impostazione della password 84
Impostazione del gruppo di età 84
Impostazione del blocco dei cookie 85
Impostazione delle limitazioni degli orari di accesso a Internet 85
Modifica di utenti 86
Modifica delle password 86

Modifica delle informazioni di un utente 86
Modifica dell'impostazione di blocco dei cookie 87
Modifica dell'elenco dei cookie accettati e rifiutati 87
Modifica del gruppo di età 88
Modifica delle limitazioni degli orari di accesso a Internet 88
Modifica dell'utente di avvio 89
Rimozione di utenti 89
Opzioni 89
Blocco di siti Web 89
Autorizzazione di siti Web 90
Blocco di informazioni 90
Aggiunta di informazioni 90
Modifica di informazioni 90
Rimozione di informazioni personali 91
Blocco di Web bug 91
Blocco della pubblicità 91
Autorizzazione di cookie da siti Web specifici 92
Registro eventi 92
Data e ora 92
Utente 92
Riepilogo 92
Dettagli evento 92
Salvataggio del registro corrente 93
Visualizzazione dei registri salvati 93
Utilità 93
Cancellazione definitiva di file con McAfee Shredder 94
Perché in Windows rimangono residui di file 94
Elementi che è possibile cancellare con McAfee Shredder 94
Cancellazione definitiva dei file in Esplora risorse 94
Come svuotare il Cestino di Windows 95
Personalizzazione delle impostazioni di Shredder 95
Backup del database di Privacy Service 95
Ripristino del database di backup 96
Opzioni utente 96
Modifica della password 97
Modifica del nome utente 97
Cancellazione della cache 97

Accettazione di cookie 98
Per rimuovere un sito Web dall'elenco: 98
Rifiuto di cookie 98
Per rimuovere un sito Web dall'elenco: 98

5 McAfee SpamKiller 99

Funzioni 99
Opzioni utente 100
Filtri 100
Informazioni sul riquadro superiore 100
Disattivazione di SpamKiller 101
Informazioni sulla pagina Riepilogo 101
Integrazione con Microsoft Outlook e Outlook Express 102
Gestione degli utenti e degli account di posta elettronica 103
Aggiunta di account di posta elettronica 103
Come indicare al programma il client di posta elettronica 104
Eliminazione di account di posta elettronica 104
Eliminazione di un account di posta elettronica da SpamKiller 105
Modifica delle proprietà degli account di posta elettronica 105
Account POP3 105
Account MSN/Hotmail 107
Account MAPI 109
Aggiunta di utenti 110
Password utente e protezione dei minori dai messaggi indesiderati 112
Accesso a SpamKiller in un ambiente multiutente 113
Utilizzo dell'elenco degli amici 114
Apertura di un elenco degli amici 115
Importazione di rubriche 115
Importazione automatica di una rubrica 116
Importazione manuale di una rubrica 116
Modifica delle informazioni di una rubrica 117
Eliminazione di rubriche dall'elenco di importazione automatica 117
Aggiunta di amici 117
Aggiunta di amici dalla pagina Posta bloccata o Posta accettata 118
Aggiunta di amici dalla pagina Amici 118
Aggiunta di amici da Microsoft Outlook 119
Modifica di amici 119
Eliminazione di amici 120

Utilizzo dei messaggi bloccati e accettati 120
Pagina Posta bloccata 121
Pagina Posta accettata 122
Operazioni relative alla posta bloccata e accettata 123
Ripristino di messaggi 124
Dalla pagina Posta bloccata 124
Dalla cartella SpamKiller in Microsoft Outlook o da Outlook Express 124
Blocco di messaggi 125
Dalla pagina Posta accettata 125
Da Microsoft Outlook 125
Dove sono i messaggi bloccati 125
Eliminazione manuale di un messaggio 126
Modifica della modalità di elaborazione dei messaggi indesiderati 126
Assegnazione di contrassegni 126
Blocco 126
Modifica della modalità di elaborazione dei messaggi indesiderati 127
Utilizzo di AntiPhishing Filter 127
Aggiunta di amici a un elenco degli amici 128
Aggiunta di filtri 128
Espressioni regolari (RegEx) 130
Segnalazione dei messaggi indesiderati a McAfee 133
Invio manuale di reclami 133
Invio di messaggi di errore 134
Invio manuale di un messaggio di errore: 134

Indice 135

Introduzione 1

Internet offre una grande quantità di informazioni e attività di intrattenimento a portata di mouse. Tuttavia, appena ci si collega, si espone il computer a un gran numero di minacce per la sicurezza e la riservatezza. McAfee Internet Security Suite consente di proteggere la privacy degli utenti e i dati presenti sul computer. Grazie alle tecnologie d'avanguardia di McAfee, Internet Security Suite costituisce uno dei pacchetti più completi per la protezione della privacy e della sicurezza disponibili sul mercato. McAfee Internet Security Suite elimina i virus, neutralizza gli hacker, protegge le informazioni personali, tutela la riservatezza della navigazione sul Web, blocca la pubblicità e le finestre popup, gestisce i cookie e le password, blocca l'accesso a file, cartelle e unità, filtra il contenuto non gradito e consente all'utente di controllare il traffico Internet in arrivo e in uscita dal computer.

McAfee Internet Security Suite è un'affidabile soluzione di protezione che tutela completamente gli utenti di Internet.

McAfee Internet Security Suite include i seguenti prodotti:

- *McAfee VirusScan* a pagina 15
- *McAfee Personal Firewall Plus* a pagina 49
- *McAfee Privacy Service* a pagina 81
- *McAfee SpamKiller* a pagina 99

Software McAfee Internet Security

- **McAfee SecurityCenter:** valuta, informa e avvisa l'utente in merito alla vulnerabilità del computer in termini di protezione. Ogni indice di protezione permette di valutare velocemente l'esposizione alle minacce provenienti da Internet e fornisce i suggerimenti per proteggere il computer in modo rapido e sicuro.
- **McAfee VirusScan:** ricerca, rileva, ripara e rimuove i file con virus provenienti da Internet. È possibile personalizzare le scansioni e determinare le opzioni di risposta e le azioni da intraprendere quando viene rilevato un virus. È inoltre possibile configurare VirusScan per registrare le azioni relative ai virus eseguite sul computer.
- **McAfee Personal Firewall Plus:** protegge il computer durante la connessione e il traffico Internet in arrivo e in uscita dal computer.
- **McAfee Privacy Service:** combina la protezione delle informazioni personali con il blocco della pubblicità e il filtraggio dei contenuti. Questo servizio protegge le informazioni personali dell'utente e nel contempo offre un maggior controllo sull'uso di Internet in famiglia. McAfee Privacy Service garantisce che le informazioni riservate non vengano esposte a minacce online e protegge utenti e familiari da contenuti ritenuti inadeguati.
- **McAfee SpamKiller:** con l'aumento dei messaggi a scopo di frode, importuni e offensivi che adulti, bambini e aziende ricevono, la protezione dalla posta indesiderata diventa una componente essenziale della strategia di protezione del computer.

Requisiti di sistema

- Microsoft® Windows 98, Me, 2000 o XP
- PC con processore compatibile Pentium
  - Windows 98, 2000: 133 MHz o superiore
  - Windows Me: 150 MHz o superiore
  - Windows XP (Home e Pro): 300 MHz o superiore
- RAM
  - Windows 98, Me, 2000: 64 MB
  - Windows XP (Home e Pro): 128 MB
- 100 MB di spazio libero su disco rigido
- Microsoft® Internet Explorer 5.5 o versione successiva

NOTA: Per eseguire l'aggiornamento all'ultima versione di Internet Explorer, visitare il sito Web di Microsoft, all'indirizzo http://www.microsoft.com.

Utilizzo di McAfee SecurityCenter

McAfee SecurityCenter è un punto di riferimento singolo per la protezione, accessibile dalla relativa icona nella barra delle applicazioni di Windows oppure dal desktop di Windows. McAfee SecurityCenter consente di eseguire le seguenti operazioni utili:

- Ottenere l'analisi gratuita del grado di protezione del computer.
- Avviare, gestire e configurare tutti gli abbonamenti a McAfee utilizzando un'unica icona.
- Vedere avvisi sui virus costantemente aggiornati e le ultimissime informazioni sui prodotti.
- Ottenere collegamenti rapidi alle domande frequenti e informazioni sugli account nel sito Web di McAfee.

> **NOTA**
> Per ulteriori informazioni sulle funzioni di SecurityCenter, fare clic su **Guida** nella finestra di dialogo **SecurityCenter**.

Quando SecurityCenter è in esecuzione e tutte le funzioni di McAfee installate nel computer sono attivate, nella barra delle applicazioni di Windows viene visualizzata un'icona raffigurante una **M** rossa . Quest'area si trova in genere nell'angolo inferiore destro del desktop di Windows e contiene l'orologio.

In caso di disattivazione di una o più applicazioni McAfee installate nel computer, l'icona McAfee risulterà di colore nero .

Per aprire McAfee SecurityCenter:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows.
2. Fare clic su **Apri SecurityCenter**.

Per accedere al prodotto McAfee desiderato:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows.
2. Scegliere il prodotto McAfee desiderato e selezionare la funzione da utilizzare.

Rimozione dei programmi di Internet Security Suite

In alcuni casi, potrebbe essere necessario rimuovere Internet Security Suite o alcuni dei programmi della suite.

NOTA
Per disinstallare Internet Security Suite occorre disporre dei privilegi di amministratore.

1. Salvare le eventuali modifiche effettuate e chiudere tutte le applicazioni aperte.
2. Aprire il **Pannello di controllo**.
   - Nella barra delle applicazioni di Windows, selezionare **Start**, scegliere **Impostazioni**, quindi fare clic su **Pannello di controllo** (Windows 98, 2000).
   - Nella barra delle applicazioni di Windows, selezionare **Start**, quindi fare clic su **Pannello di controllo** (Windows XP).
3. Fare clic su **Installazione applicazioni**.
4. Selezionare Disinstallazione guidata di McAfee, i programmi che si desidera disintallare, quindi fare clic su **Rimuovi**.
5. Fare clic su **Sì** per procedere con la rimozione.
6. Sarà richiesto di riavviare il computer.

McAfee VirusScan 2

Benvenuti in McAfee VirusScan.

McAfee VirusScan è un servizio antivirus ad abbonamento che offre una protezione antivirus completa, affidabile e aggiornata. Basato sulla notissima tecnologia di scansione di McAfee, VirusScan protegge da virus, worm, cavalli di Troia, script dannosi e attacchi di pirati informatici.

Grazie a questo software, è possibile usufruire delle seguenti funzioni:

ActiveShield: esegue la scansione dei file quando vengono aperti dall'utente o dal computer.

Funzione Scansione: ricerca virus e programmi potenzialmente indesiderati nei dischi rigidi, nei dischi floppy e nei singoli file e cartelle.

Quarantena: crittografia e isolamento temporaneo nella cartella di quarantena dei file infetti e sospetti fino a quando non è possibile effettuare le operazioni appropriate.

Rilevamento di attività ostili: controllo nel computer di attività di tipo virale causate da script dannosi e attività simili a worm.

Nuove funzioni

Questa versione di VirusScan offre le nuove funzioni indicate di seguito:

- **Rilevamento e rimozione di spyware e adware**
  VirusScan identifica e rimuove spyware, adware e altri programmi in grado di compromettere la privacy e rallentare le prestazioni del computer.
- **Aggiornamenti automatici giornalieri**
  Gli aggiornamenti automatici di VirusScan consentono di aggiornare la protezione del computer nei confronti delle più recenti minacce identificate e non identificate.
- **Scansione in background**
  Veloci scansioni identificano e distruggono con discrezione virus, cavalli di Troia, worm, spyware, adware, dialer e altri programmi dannosi senza interrompere il lavoro dell'utente.
- **Avvisi di protezione in tempo reale**
  Gli avvisi di protezione notificano all'utente la presenza di epidemie di virus e minacce di protezione e forniscono opzioni di risposta che consentono di rimuovere, neutralizzare o conoscere meglio la minaccia.

- **Rilevamento e pulizia in più punti di accesso**
  VirusScan esegue il monitoraggio e la pulizia nei principali punti di accesso del computer: messaggi di posta elettronica, allegati di messaggi immediati e download di Internet.

- **Monitoraggio della posta elettronica per attività simili a worm**
  WormStopper™ esegue il monitoraggio delle operazioni sospette di mass-mailing e impedisce che virus e worm si diffondano in altri computer tramite posta elettronica.

- **Monitoraggio degli script per attività simili a worm**
  ScriptStopper™ esegue il monitoraggio di operazioni sospette di esecuzione di script e impedisce che virus e worm si diffondano in altri computer tramite posta elettronica.

- **Supporto tecnico gratuito tramite posta elettronica e messaggistica immediata**
  Il supporto tecnico dal vivo fornisce assistenza in maniera semplice e tempestiva tramite posta elettronica e messaggistica immediata.

Verifica di VirusScan

Prima di utilizzare VirusScan per la prima volta, è consigliabile verificare l'installazione. Attenersi alla seguente procedura per verificare separatamente le funzioni ActiveShield e di scansione.

Verifica di ActiveShield

NOTA
Per verificare ActiveShield dalla scheda VirusScan in SecurityCenter, fare clic su **Prova VirusScan** per visualizzare le domande frequenti online di supporto contenenti questa procedura.

Per verificare ActiveShield:

1. Aprire il browser Web e accedere al sito http://www.eicar.com/.
2. Fare clic sul collegamento **The AntiVirus testfile eicar.com**.
3. Scorrere fino in fondo alla pagina. In **Download** sono disponibili quattro collegamenti.
4. Fare clic su **eicar.com**.

Se ActiveShield funziona correttamente, il file eicar.com verrà rilevato immediatamente appena si fa clic sul collegamento. È possibile provare a eliminare o mettere in quarantena i file infetti per vedere in che modo ActiveShield gestisce i virus. Per ulteriori informazioni, vedere la sezione *Informazioni suli avvisi di protezione* a pagina 29.

Verifica della funzione Scansione

Prima di poter verificare la funzione Scansione, è necessario disattivare ActiveShield per evitare che rilevi i file infetti prima della funzione di scansione e quindi scaricare i file di prova.

Per scaricare i file di prova:

1. Disattivare ActiveShield: fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Disattiva**.
2. Scaricare i file di prova EICAR dal sito Web della EICAR:
   a. Accedere al sito http://www.eicar.com/.
   b. Fare clic sul collegamento **The AntiVirus testfile eicar.com**.

c Scorrere fino in fondo alla pagina. In **Download** sono disponibili questi collegamenti:

eicar.com contiene una riga di testo che viene rilevata come virus da VirusScan.

eicar.com.txt (opzionale) è lo stesso file, ma con un nome diverso, per gli utenti che hanno difficoltà a scaricare il primo. Rinominare semplicemente il file in "eicar.com" una volta scaricato.

eicar_com.zip è una copia del virus di prova in un file compresso .ZIP, ossia un archivio di file WinZip™.

eicarcom2.zip è una copia del virus di prova in un file compresso .ZIP, che a sua volta si trova in un file compresso .ZIP.

d Fare clic su ogni collegamento per scaricare il rispettivo file. Per ciascun file viene visualizzata la finestra di dialogo **Download file**.

e Fare clic su **Salva**, selezionare il pulsante **Crea nuova cartella** e rinominare la cartella **Cartella scansione VSO**.

f Fare doppio clic sulla **Cartella scansione VSO**, quindi selezionare nuovamente **Salva** in ogni finestra di dialogo **Salva con nome**.

3 Al termine del download dei file, chiudere Internet Explorer.

4 Attivare ActiveShield: fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Attiva**.

Per verificare la funzione di scansione:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Ricerca virus**.

2 Utilizzando la struttura delle directory nel riquadro di sinistra della finestra di dialogo, andare alla cartella **Cartella scansione VSO** in cui erano stati salvati i file:

a Fare clic sul segno **+** accanto all'icona dell'unità C.

b Fare clic su **Cartella scansione VSO** per evidenziare tale cartella. Non fare clic sul segno **+** accanto alla cartella.

In questo modo la ricerca dei virus viene eseguita solo nella cartella specificata. In alternativa, è possibile spostare i file in posizioni casuali nel disco rigido per ottenere una dimostrazione più convincente delle capacità della funzione di scansione.

3 Nell'area **Opzioni di scansione** della finestra di dialogo **Ricerca virus**, assicurarsi che tutte le opzioni siano selezionate.

4 Fare clic su **Scansione** nella parte inferiore della finestra di dialogo.

VirusScan esegue la scansione di **Cartella scansione VSO**. I file di prova EICAR salvati in quella cartella vengono visualizzati in **Elenco dei file rilevati**. In tal caso, la scansione funziona correttamente.

È possibile provare a eliminare o mettere in quarantena i file infetti per vedere come vengono gestiti i virus dalla funzione di scansione. Per ulteriori informazioni, vedere la sezione *Informazioni sul rilevamento delle minacce* a pagina 39.

Utilizzo di ActiveShield

Quando viene avviato (caricato nella memoria del computer) e attivato, ActiveShield protegge costantemente il computer. ActiveShield esegue la scansione dei file quando vengono aperti dall'utente o dal computer. Quando ActiveShield rileva un file che contiene un virus, cerca automaticamente di pulirlo. Se questa operazione non riesce, è possibile mettere in quarantena o eliminare il file.

Attivazione o disattivazione di ActiveShield

ActiveShield viene avviato (caricato nella memoria del computer) e attivato (indicato dall'icona rossa nella barra delle applicazioni di Windows) per impostazione predefinita appena si riavvia il computer al termine dell'installazione.

Se ActiveShield viene interrotto (non caricato) o è disattivato (indicato dall'icona nera), sarà possibile eseguirlo manualmente o configurarne l'esecuzione automatica all'avvio di Windows.

Attivazione di ActiveShield

Per attivare ActiveShield solo per questa sessione di Windows:

Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Attiva**. L'icona McAfee diventa di colore rosso .

Se ActiveShield è ancora configurato per essere avviato all'avvio di Windows, verrà visualizzato un messaggio che indica che ora la protezione dai virus è attiva. In caso contrario, verrà visualizzata una finestra di dialogo che consente di configurare l'avvio di ActiveShield all'avvio di Windows (Figura 2-1 a pagina 20).

Disattivazione di ActiveShield

Per disattivare ActiveShield solo per questa sessione di Windows:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Disattiva**.
2. Fare clic su **Sì** per confermare.

   L'icona McAfee diventa di colore nero .

Se ActiveShield è ancora configurato per essere avviato all'avvio di Windows, il computer sarà protetto nuovamente dai virus quando verrà riavviato.

Configurazione delle opzioni di ActiveShield

Nella scheda **ActiveShield** della finestra di dialogo **Opzioni di VirusScan** (Figura 2-1), accessibile facendo clic sull'icona McAfee nella barra delle applicazioni di Windows, è possibile modificare le opzioni di avvio e di scansione di ActiveShield.

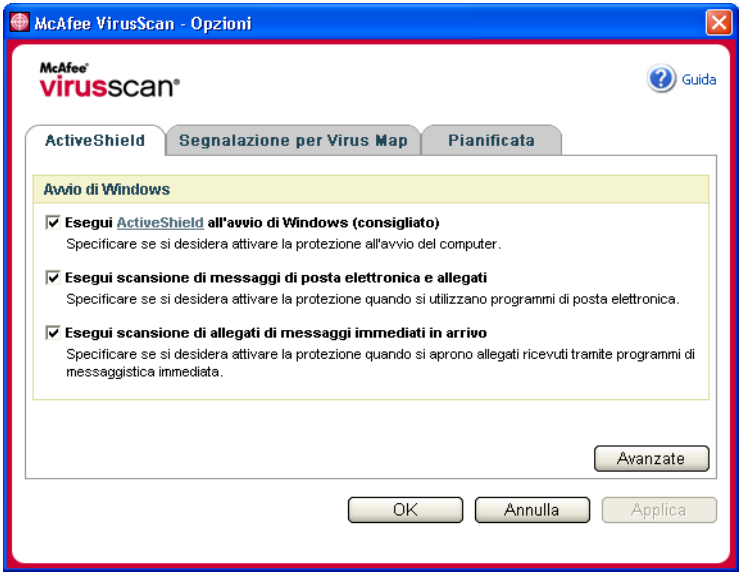

McAfee VirusScan - Opzioni
McAfee
virusscan
Guida
ActiveShield
Segnalazione per Virus Map
Pianificata
Avvio di Windows
Esegui ActiveShield all'avvio di Windows (consigliato)
Specificare se si desidera attivare la protezione all'avvio del computer.
Esegui scansione di messaggi di posta elettronica e allegati
Specificare se si desidera attivare la protezione quando si utilizzano programmi di posta elettronica.
Esegui scansione di allegati di messaggi immediati in arrivo
Specificare se si desidera attivare la protezione quando si aprono allegati ricevuti tramite programmi di messaggistica immediata.
Avanzate
OK
Annulla
Applica

Figura 2-1. Opzioni di ActiveShield

Avvio di ActiveShield

ActiveShield viene avviato (caricato nella memoria del computer) e attivato (indicato dall'icona rossa) per impostazione predefinita appena si riavvia il computer al termine dell'installazione.

Se ActiveShield non è attivato (indicato dall'icona nera), è possibile configurarne l'avvio automatico all'avvio di Windows (consigliato).

> **NOTA**
> Durante gli aggiornamenti di VirusScan, ActiveShield potrebbe venire temporaneamente disattivato dalla **procedura guidata di aggiornamento** per consentire l'installazione dei nuovi file. Quando nella **procedura guidata di aggiornamento** viene chiesto di fare clic su **Fine**, ActiveShield viene riavviato.

Per avviare ActiveShield automaticamente all'avvio di Windows:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.

   Verrà visualizzata la finestra di dialogo **Opzioni di VirusScan** (Figura 2-1 a pagina 20).

2. Selezionare la casella di controllo **Esegui ActiveShield all'avvio di Windows (consigliato)**, quindi fare clic su **Applica** per salvare le modifiche.

3. Fare clic su **OK** per confermare, quindi nuovamente su **OK**.

Arresto di ActiveShield

> **ATTENZIONE**
> Se si arresta ActiveShield, il computer non sarà protetto dai virus. Se occorre arrestare ActiveShield, salvo quando si aggiorna VirusScan, accertarsi di non essere connessi a Internet.

Per interrompere l'avvio automatico di ActiveShield all'avvio di Windows:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.

   Verrà visualizzata la finestra di dialogo **Opzioni di VirusScan** (Figura 2-1 a pagina 20).

2. Deselezionare la casella di controllo **Esegui ActiveShield all'avvio di Windows (consigliato)**, quindi fare clic su **Applica** per salvare le modifiche.

3. Fare clic su **OK** per confermare, quindi nuovamente su **OK**.

Scansione di messaggi di posta elettronica e allegati

Per impostazione predefinita, l'opzione **Esegui scansione di messaggi di posta elettronica e allegati** (Figura 2-1 a pagina 20) è attivata.

Quando questa opzione è attivata, ActiveShield esegue automaticamente la scansione e tenta di pulire i messaggi di posta elettronica e gli allegati infetti in ingresso (POP3) e in uscita (SMTP) per i client di posta elettronica più diffusi, tra cui:

- Microsoft Outlook Express 4.0 o versioni successive
- Microsoft Outlook 97 o versioni successive
- Netscape Messenger 4.0 o versioni successive
- Netscape Mail 6.0 o versioni successive
- Eudora Light 3.0 o versioni successive
- Eudora Pro 4.0 o versioni successive
- Eudora 5.0 o versioni successive
- Pegasus 4.0 o versioni successive

NOTA

La scansione della posta elettronica non è supportata per i seguenti client: client basati su Web, IMAP, AOL, POP3 SSL e Lotus Notes. Tuttavia, ActiveShield analizza gli allegati di posta elettronica quando vengono aperti.

Se si disattiva l'opzione **Esegui scansione di messaggi di posta elettronica e allegati**, le opzioni di scansione e le opzioni di WormStopper (Figura 2-2 a pagina 23) vengono disattivate automaticamente. Se si disattiva la scansione dei messaggi di posta elettronica in uscita, le opzioni di WormStopper vengono disattivate automaticamente.

Se si modificano le opzioni di scansione posta, è necessario riavviare il programma di posta elettronica per completare le modifiche.

Messaggi di posta elettronica in ingresso

Se un messaggio di posta elettronica o un allegato in ingresso sono infetti, ActiveShield esegue le seguenti operazioni:

- Tenta di pulire il messaggio infetto
- Tenta di mettere in quarantena o eliminare un messaggio che non è possibile pulire
- Include nel messaggio in ingresso un file di avviso che contiene informazioni sulle azioni eseguite per rimuovere l'infezione

Messaggi di posta elettronica in uscita

Se un messaggio di posta elettronica o un allegato in uscita sono infetti, ActiveShield esegue le seguenti operazioni:

- Tenta di pulire il messaggio infetto
- Tenta di mettere in quarantena o eliminare un messaggio che non è possibile pulire

> **NOTA**
> Per informazioni sugli errori di scansione dei messaggi di posta elettronica in uscita, vedere la Guida in linea.

Disattivazione della scansione della posta elettronica

Per impostazione predefinita, ActiveShield esegue la scansione dei messaggi di posta elettronica in ingresso e in uscita. Tuttavia, per un controllo migliore è possibile impostare ActiveShield in modo che effettui solo la scansione dei messaggi di posta elettronica in ingresso o in uscita.

Per disattivare la scansione dei messaggi di posta elettronica in ingresso o in uscita:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.
2. Fare clic su **Avanzate**, quindi sulla scheda **Scans. posta** (Figura 2-2).
3. Deselezionare **Messaggi e-mail in ingresso** o **Messaggi e-mail in uscita**, quindi fare clic su **OK**.

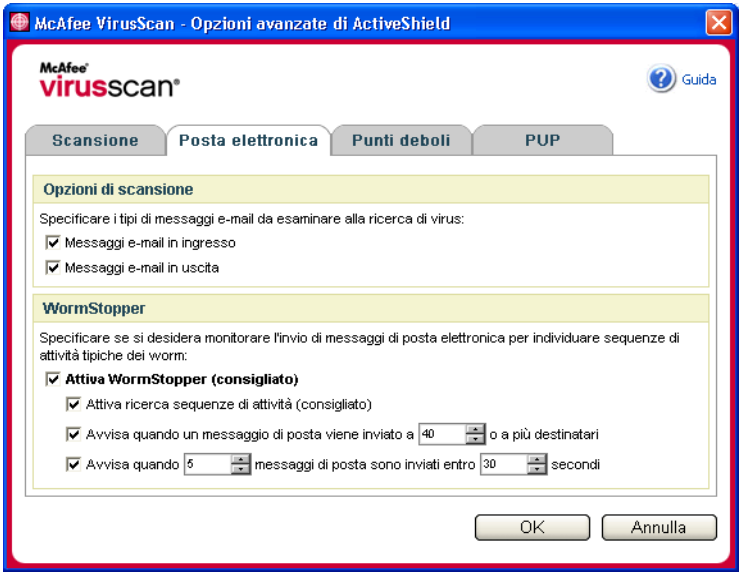

McAfee VirusScan - Opzioni avanzate di ActiveShield
McAfee
virusscan
Guida
Scansione
Posta elettronica
Punti deboli
PUP
Opzioni di scansione
Specificare i tipi di messaggi e-mail da esaminare alla ricerca di virus:
Messaggi e-mail in ingresso
Messaggi e-mail in uscita
WormStopper
Specificare se si desidera monitorare l'invio di messaggi di posta elettronica per individuare sequenze di attività tipiche dei worm:
Attiva WormStopper (consigliato)
Attiva ricerca sequenze di attività (consigliato)
Avvisa quando un messaggio di posta viene inviato a 40 o a più destinatari
Avvisa quando 6 messaggi di posta sono inviati entro 30 secondi
OK
Annulla

Figura 2-2. Opzioni avanzate di ActiveShield - Scheda Posta elettronica

Ricerca di worm

VirusScan controlla eventuali attività sospette del computer che potrebbero indicare la presenza di una minaccia. VirusScan pulisce i virus, mentre WormStopper™ impedisce l'ulteriore diffusione di virus e worm.

Un "worm" è un virus in grado di autoreplicarsi; esso risiede nella memoria attiva e può inviare copie di se stesso attraverso la posta elettronica. Senza WormStopper, è possibile notare i worm solo quando l'attività incontrollata di duplicazione consuma le risorse del sistema, rallentando le prestazioni o interrompendo le attività.

Il meccanismo di protezione di WormStopper rileva, avvisa e blocca le attività dannose. Le attività sospette nel computer potrebbero includere:

- Il tentativo di inoltrare un messaggio di posta elettronica a un gran numero di utenti presenti nella propria rubrica
- Tentativi di inoltrare più messaggi di posta elettronica in rapida successione

Se si imposta ActiveShield in modo da utilizzare l'opzione **Attiva WormStopper (consigliato)** nella finestra di dialogo **Opzioni avanzate**, WormStopper controllerà l'attività della posta elettronica alla ricerca di sequenze sospette e avviserà l'utente se viene superato un numero specifico di messaggi o destinatari entro un dato intervallo di tempo.

Per impostare ActiveShield in modo che venga eseguita la scansione dei messaggi di posta elettronica inviati, alla ricerca di attività simili a worm:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.
2. Fare clic su **Avanzate**, quindi sulla scheda **Posta elettronica**.
3. Fare clic su **Attiva WormStopper (consigliato)** (Figura 2-3).

   Per impostazione predefinita, sono attivate le seguenti opzioni dettagliate:

   - Ricerca di sequenze di attività per rilevare quelle sospette
   - Avviso in caso di invio di messaggi di posta elettronica a 40 o più destinatari
   - Avviso in caso di invio di 5 o più messaggi di posta elettronica entro 30 secondi

     NOTA
     Se si modifica il numero di destinatari o di secondi per il monitoraggio dei messaggi di posta elettronica inviati, è possibile che si verifichino rilevamenti non validi. McAfee consiglia di selezionare **No** per mantenere l'impostazione predefinita. In caso contrario, selezionare **Sì** per personalizzare l'impostazione predefinita.

È possibile attivare automaticamente questa opzione dopo il primo rilevamento di un potenziale worm (per ulteriori informazioni, vedere la sezione *Gestione dei potenziali worm* a pagina 31):

- Blocco automatico di messaggi di posta elettronica sospetti in uscita

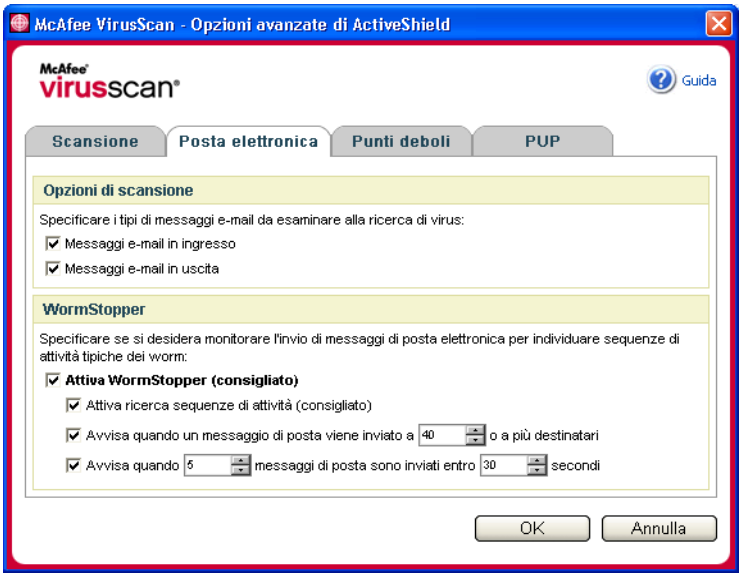

McAfee VirusScan - Opzioni avanzate di ActiveShield
McAfee
virusscan
Guida
Scansione
Posta elettronica
Punti deboli
PUP
Opzioni di scansione
Specificare i tipi di messaggi e-mail da esaminare alla ricerca di virus:
Messaggi e-mail in ingresso
Messaggi e-mail in uscita
WormStopper
Specificare se si desidera monitorare l'invio di messaggi di posta elettronica per individuare sequenze di attività tipiche dei worm:
Attiva WormStopper (consigliato)
Attiva ricerca sequenze di attività (consigliato)
Avvisa quando un messaggio di posta viene inviato a 40 o a più destinatari
Avvisa quando 5 messaggi di posta sono inviati entro 30 secondi
OK
Annulla

Figura 2-3. Opzioni avanzate di ActiveShield - Scheda Posta elettronica

Scansione degli allegati dei messaggi immediati in arrivo

Per impostazione predefinita, l'opzione **Esegui scansione di allegati di messaggi immediati in arrivo** (Figura 2-1 a pagina 20) è attivata.

Quando questa opzione è attivata, VirusScan esegue automaticamente la scansione e tenta di pulire gli allegati infetti dei messaggi immediati in ingresso per i programmi di messaggistica immediata più diffusi, tra cui:

- MSN Messenger 6.0 o versioni successive
- Yahoo Messenger 4.1 o versioni successive
- AOL Instant Messenger 2.1 o versioni successive

NOTA
Per una maggiore protezione, non è possibile disattivare la pulizia automatica degli allegati dei messaggi immediati.

Se l'allegato di un messaggio immediato in ingresso è infetto, VirusScan esegue le seguenti operazioni:

- Tenta di pulire il messaggio infetto
- Chiede se mettere in quarantena o eliminare un messaggio che non è possibile pulire

Scansione di tutti i file

Se si imposta ActiveShield in modo da utilizzare l'opzione predefinita **Tutti i file (consigliato)**, verrà eseguita la scansione di tutti i tipi di file utilizzati dal computer appena si tenta di aprirli. Questa opzione offre la scansione più accurata possibile.

Per impostare ActiveShield per eseguire la scansione di tutti i tipi di file:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.
2. Fare clic su **Avanzate**, quindi sulla scheda **Scansione** (Figura 2-4 a pagina 26).
3. Fare clic su **Tutti i file (consigliato)**, quindi su **OK**.

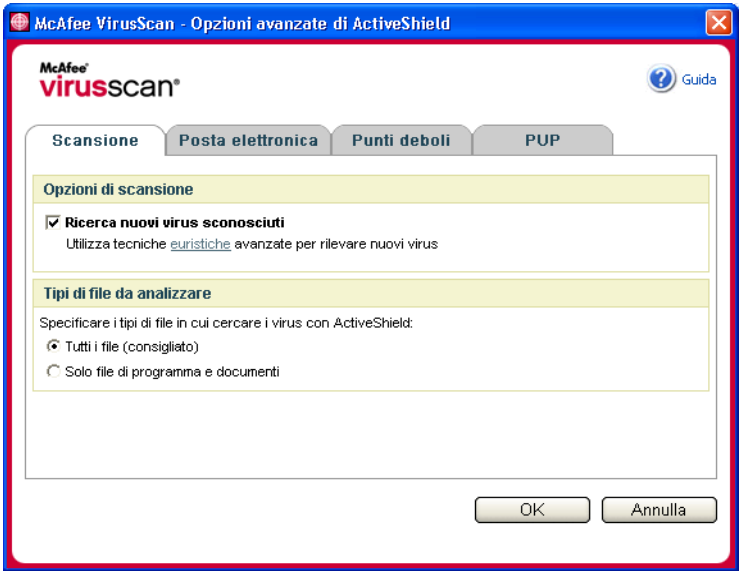


Figura 2-4. Opzioni avanzate di ActiveShield – Scheda Scansione

Scansione esclusivamente di file di programma e documenti

Se si imposta ActiveShield in modo che venga utilizzata l'opzione **Solo file di programma e documenti**, verrà eseguita la scansione dei file di programma e dei documenti, ma non di altri file in uso nel computer. I tipi di file analizzati da ActiveShield vengono determinati dal file più recente delle firme elettroniche dei virus (file DAT). Per impostare ActiveShield per analizzare solo file di programma e documenti:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.
2. Fare clic su **Avanzate**, quindi sulla scheda **Scansione** (Figura 2-4).
3. Fare clic su **Solo file di programma e documenti**, quindi su **OK**.

Ricerca di nuovi virus sconosciuti

Se si imposta ActiveShield in modo che utilizzi l'opzione predefinita **Ricerca nuovi virus sconosciuti (consigliato)**, le tecniche euristiche avanzate utilizzate da ActiveShield tentano di far corrispondere i file alle firme elettroniche di virus conosciuti, esaminando nel contempo gli indizi significativi di virus non identificati nei file.

Per impostare ActiveShield per ricercare virus nuovi e sconosciuti:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.
2. Fare clic su **Avanzate**, quindi sulla scheda **Scansione** (Figura 2-4).
3. Fare clic su **Ricerca nuovi virus sconosciuti (consigliato)**, quindi su **OK**.

Ricerca di script

VirusScan controlla eventuali attività sospette del computer che potrebbero indicare la presenza di una minaccia. VirusScan pulisce i virus, mentre ScriptStopperTM impedisce ai cavalli di Troia di eseguire script che diffondono ulteriormente i virus.

Un "cavallo di Troia" è un programma dannoso che finge di essere un'applicazione innocua. I cavalli di Troia non sono virus in quanto non duplicano se stessi, ma possono essere altrettanto distruttivi.

Il meccanismo di protezione di ScriptStopper rileva, avvisa e blocca le attività dannose. Le attività sospette nel computer potrebbero includere:

- L'esecuzione di uno script che causa la creazione, la copia o l'eliminazione di file oppure l'apertura del registro di configurazione di Windows

Se si imposta ActiveShield in modo da utilizzare l'opzione **Attiva ScriptStopper (consigliato)** nella finestra di dialogo **Opzioni avanzate**, ScriptStopper controllerà l'esecuzione degli script alla ricerca di sequenze sospette e avviserà l'utente se viene superato un numero specifico di messaggi o destinatari entro un dato intervallo di tempo.

Per impostare ActiveShield in modo che venga eseguita la scansione degli script in esecuzione alla ricerca di attività simili a worm:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.
2. Fare clic su **Avanzate**, quindi sulla scheda **Punti deboli** (Figura 2-5).

3 Fare clic su **Attiva ScriptStopper (consigliato)** quindi fare clic su **OK**.

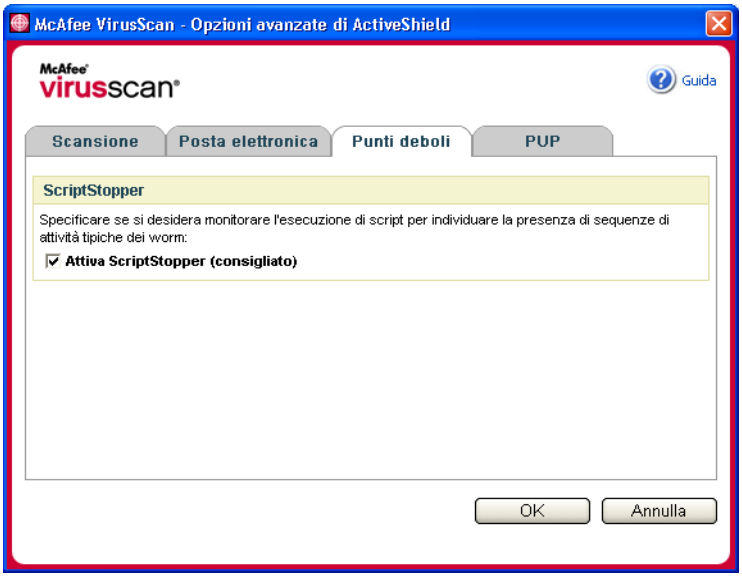


Figura 2-5. Opzioni avanzate di ActiveShield – Scheda Punti deboli

Scansione per la ricerca di programmi potenzialmente indesiderati (PUP)

NOTA
Se è installato nel computer, McAfee AntiSpyware gestisce tutte le attività dei programmi potenzialmente indesiderati. Aprire McAfee AntiSpyware per configurare le opzioni.

Se si imposta ActiveShield in modo da utilizzare l'opzione predefinita **Ricerca programmi potenzialmente indesiderati (consigliato)** nella finestra di dialogo **Opzioni avanzate**, la protezione dai programmi potenzialmente indesiderati (PUP) rileva, blocca e rimuove rapidamente spyware, adware e altro malware che raccoglie e trasmette i dati personali senza l'autorizzazione dell'utente.

Per impostare ActiveShield per eseguire la scansione dei PUP:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.

2 Fare clic su **Avanzate**, quindi sulla scheda **PUP** (Figura 2-6).

3 Fare clic su **Ricerca programmi potenzialmente indesiderati (consigliato)**, quindi su **OK**.

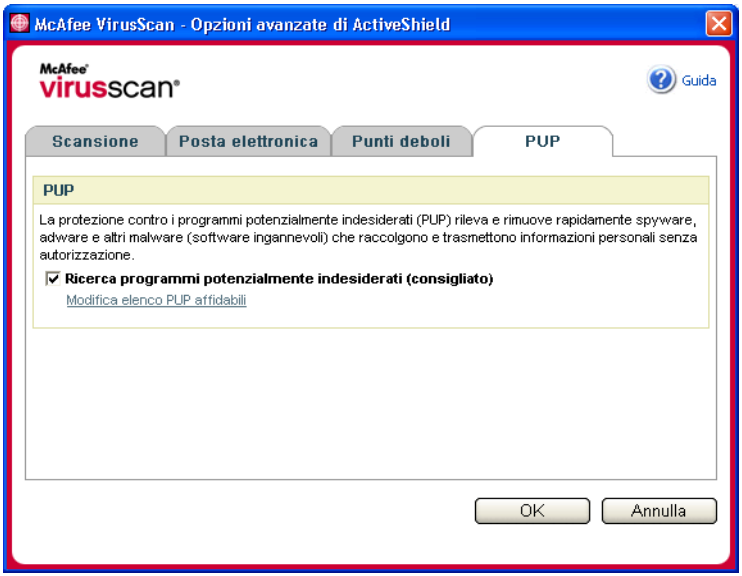


Figura 2-6. Opzioni avanzate di ActiveShield – Scheda PUP

Informazioni sui avvisi di protezione

Se ActiveShield individua un virus, verrà visualizzato un avviso simile a quello nella Figura 2-7. ActiveShield cerca automaticamente di pulire il file e avvisa l'utente per la maggior parte dei virus, cavalli di Troia e worm. Per i programmi potenzialmente indesiderati (PUP), ActiveShield rileva e blocca automaticamente il file e avvisa l'utente.

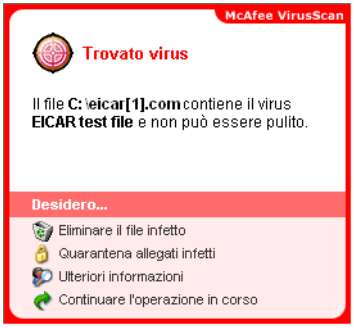

McAfee VirusScan
Trovato virus
Il file C:\eicar[1].com contiene il virus EICAR test file e non può essere pulito.
Desidero...
Eliminare il file infetto
Quarantena allegati infetti
Ulteriori informazioni
Continuare l'operazione in corso

Figura 2-7. Avviso di virus

È possibile tuttavia scegliere come gestire i file infetti, i messaggi di posta elettronica infetti, gli script sospetti, i potenziali worm o i PUP, nonché decidere se inviare i file infetti ai laboratori AVERT di McAfee affinché vengano analizzati.

Per aumentare il livello di protezione, ogni volta che ActiveShield rileva un file sospetto, viene richiesto all'utente di eseguire immediatamente la scansione dell'intero computer. Se non si sceglie di nascondere la richiesta di scansione, verrà visualizzato periodicamente un promemoria fino a quando si decide di eseguire la scansione.

Gestione dei file infetti

1. Se ActiveShield è in grado di pulire il file, è possibile visualizzare ulteriori informazioni o ignorare l'avviso:
   - Fare clic su **Ulteriori informazioni** per visualizzare il nome, il percorso e il nome del virus associati al file infetto.
   - Fare clic su **Continuare l'operazione in corso** per ignorare e chiudere l'avviso.
2. Se ActiveShield non è in grado di pulire il file, fare clic su **Mettere in quarantena file infetto** per crittografare e isolare temporaneamente nella directory di quarantena i file infetti o sospetti, fino a quando non sarà possibile effettuare le operazioni appropriate.

   Verrà visualizzato un messaggio di conferma e verrà chiesto di cercare i virus nel computer. Fare clic su **Scansione** per completare il processo di quarantena.
3. Se ActiveShield non è in grado di mettere in quarantena il file, fare clic su **Eliminare il file infetto** per cercare di rimuoverlo.

Gestione dei messaggi di posta elettronica infetti

Per impostazione predefinita, la funzione di scansione della posta elettronica tenta automaticamente di pulire i messaggi di posta elettronica infetti. Un file di avviso incluso nel messaggio in entrata notifica all'utente se il messaggio di posta elettronica è stato pulito, messo in quarantena o eliminato.

Gestione degli script sospetti

Se ActiveShield rileva uno script sospetto, è possibile visualizzare ulteriori informazioni, quindi arrestare lo script se non si intendeva avviarlo:

- Fare clic su **Ulteriori informazioni** per visualizzare il nome, il percorso e la descrizione dell'attività associati allo script sospetto.
- Fare clic su **Interrompere lo script** per evitare l'esecuzione dello script sospetto.

Se si è certi dell'affidabilità dello script, è possibile consentirne l'esecuzione:

- Fare clic su **Consentire esecuzione script** per consentire a tutti gli script contenuti in un singolo file di essere eseguiti una volta.
- Fare clic su **Continuare l'operazione in corso** per ignorare l'avviso e consentire l'esecuzione dello script.

Gestione dei potenziali worm

Se ActiveShield rileva un potenziale worm, è possibile visualizzare ulteriori informazioni, quindi arrestare l'attività di posta elettronica se non si intendeva avviarla:

- Fare clic su **Ulteriori informazioni** per visualizzare l'elenco dei destinatari, la riga dell'oggetto, il corpo del messaggio e la descrizione dell'attività sospetta associata al messaggio di posta elettronica infetto.
- Fare clic su **Interrompere questo messaggio di posta elettronica** per evitare l'invio del messaggio sospetto e per eliminarlo dalla coda dei messaggi.

Se si è certi dell'affidabilità dell'attività di posta elettronica, fare clic su **Continuare l'operazione in corso** per ignorare l'avviso e consentire l'avvio del messaggio.

Gestione dei PUP

Se ActiveShield rileva e blocca un programma potenzialmente indesiderato (PUP), è possibile visualizzare ulteriori informazioni, quindi rimuovere il programma se non si intendeva installarlo:

- Fare clic su **Ulteriori informazioni** per visualizzare il nome, il percorso e l'azione consigliata associati al PUP.
- Fare clic su **Rimuovi questo PUP** per rimuovere il programma se non si intendeva installarlo.

  Verrà visualizzato un messaggio di conferma.

  - Se l'utente (a) non riconosce il PUP o (b) non ha installato il PUP come parte di un pacchetto software o non ha accettato un contratto di licenza relativo a tali programmi, fare clic su **OK** per rimuovere il programma utilizzando il metodo di rimozione di McAfee.

  - In caso contrario, fare clic su **Annulla** per chiudere il processo di rimozione automatico. Se in seguito si cambia idea, è possibile rimuovere manualmente il programma utilizzando il relativo programma di disinstallazione.
- Fare clic su **Continuare l'operazione in corso** per ignorare l'avviso e bloccare il programma questa volta.

Se l'utente (a) riconosce il PUP o (b) ha installato il PUP come parte di un pacchetto software o ha accettato un contratto di licenza relativo a tali programmi, è possibile consentirne l'esecuzione:

- Fare clic su **Accetta come affidabile questo PUP** per autorizzare il programma e consentirne l'esecuzione in futuro.

  Per ulteriori informazioni, vedere la sezione *Gestione dei PUP affidabili*.

Gestione dei PUP affidabili

I programmi aggiunti all'elenco dei PUP affidabili non verranno rilevati da McAfee VirusScan.

Se un PUP viene rilevato e aggiunto all'elenco dei PUP affidabili, è possibile rimuoverlo in seguito dall'elenco, se necessario.

Se l'elenco dei PUP affidabili è completo, rimuovere alcune voci prima di potere considerare come affidabile un altro PUP.

Per rimuovere un programma dall'elenco dei PUP affidabili:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.
2. Fare clic su **Avanzate**, quindi sulla scheda **PUP**.
3. Fare clic su **Modifica elenco PUP affidabili**, selezionare la casella di controllo in corrispondenza del nome del file e fare clic su **Rimuovi**. Al termine della rimozione delle voci, fare clic su **OK**.

Scansione manuale del computer

La funzione Scansione consente di cercare in modo selettivo virus e programmi potenzialmente indesiderati nei dischi rigidi, nei dischi floppy e nei singoli file e cartelle. Quando viene individuato un file infetto, la funzione di scansione tenta automaticamente di pulire il file, a meno che non si tratti di un programma potenzialmente indesiderato. Se questa operazione non riesce, il file verrà messo in quarantena o eliminato.

Ricerca manuale di virus e altre minacce

Per eseguire la scansione del computer:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Ricerca virus**.

Verrà aperta la finestra di dialogo **Ricerca virus** (Figura 2-8).

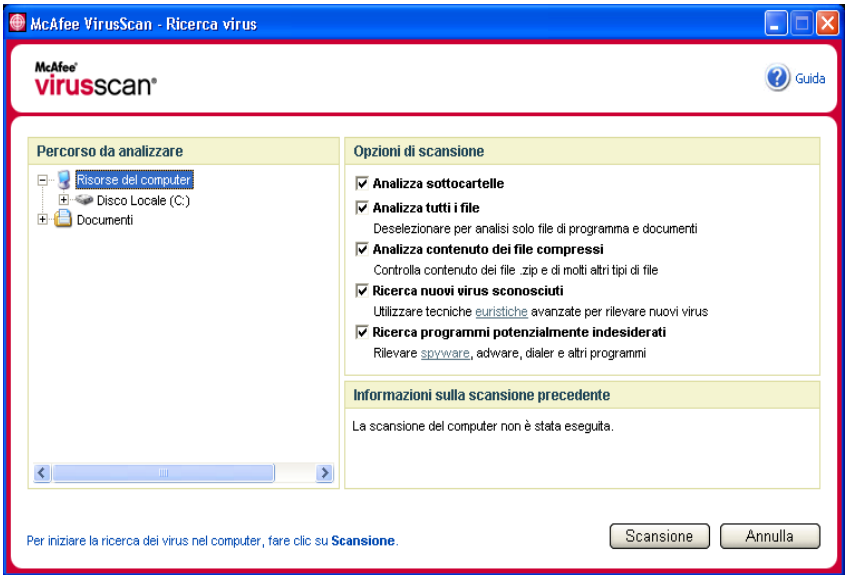

McAfee VirusScan - Ricerca virus
McAfee
virusscan
Guida
Percorso da analizzare
Risorse del computer
Disco Locale (C:)
Documenti
Opzioni di scansione
Analizza sottocartelle
Analizza tutti i file
Deselezionare per analisi solo file di programma e documenti
Analizza contenuto dei file compressi
Controlla contenuto dei file .zip e di molti altri tipi di file
Ricerca nuovi virus sconosciuti
Utilizzare tecniche euristiche avanzate per rilevare nuovi virus
Ricerca programmi potenzialmente indesiderati
Rilevare spyware, adware, dialer e altri programmi
Informazioni sulla scansione precedente
La scansione del computer non è stata eseguita.
Per iniziare la ricerca dei virus nel computer, fare clic su Scansione.
Scansione
Annulla

Figura 2-8. Finestra di dialogo Ricerca virus

2 Fare clic sull'unità, sulla cartella o sul file di cui si desidera effettuare la scansione.

3 Selezionare le **Opzioni di scansione**. Per impostazione predefinita, tutte le **Opzioni di scansione** sono preselezionate per offrire la scansione più accurata possibile (Figura 2-8):

- **Analizza sottocartelle**: questa opzione consente di eseguire la scansione dei file contenuti nelle sottocartelle. Deselezionare questa casella di controllo per consentire il controllo dei soli file visibili quando si apre una cartella o un'unità.

  Esempio: i file nella Figura 2-9 sono i soli file analizzati se si deseleziona la casella di controllo **Analizza sottocartelle**. In questo caso le cartelle e il relativo contenuto non vengono analizzati. Per eseguirne la scansione è necessario lasciare selezionata la casella di controllo.

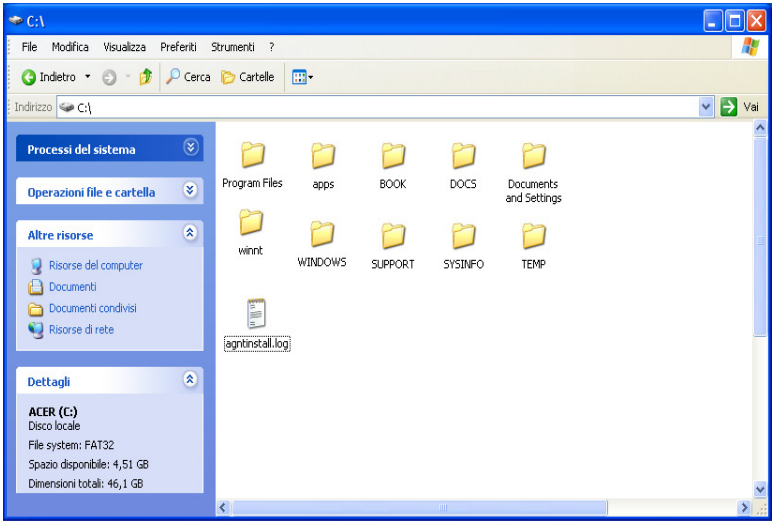


Figura 2-9. Contenuto del disco locale

- **Analizza tutti i file**: questa opzione consente di eseguire una scansione accurata di tutti i tipi di file. Deselezionare questa casella di controllo per ridurre i tempi di scansione e consentire solo la scansione dei file di programma e dei documenti.
- **Analizza contenuto dei file compressi**: questa opzione consente di rilevare file infetti nascosti nei file .ZIP e in altri file compressi. Deselezionare questa casella di controllo per evitare l'analisi dei file compressi o dei file contenuti nei file compressi.

  Talvolta gli autori dei virus inseriscono i virus in un file .ZIP, quindi inseriscono questo file .ZIP in un altro file .ZIP nel tentativo di superare le barriere dei programmi antivirus. La selezione della presente opzione consente di rilevare anche questi virus.

- **Ricerca nuovi virus sconosciuti**: questa opzione consente di trovare i virus più recenti per i quali potrebbe ancora non essere disponibile un rimedio. Utilizza tecniche euristiche avanzate che tentano di far corrispondere i file alle firme elettroniche di virus conosciuti, esaminando nel contempo gli indizi significativi di virus non identificati nei file.

  Questo metodo di scansione esamina anche le caratteristiche dei file che in genere indicano la presenza di un virus. In questo modo, le possibilità di un'indicazione errata sono ridotte al minimo. In ogni caso, se viene rilevato un virus con una scansione euristica, è consigliabile trattare il file con le stesse precauzioni che si applicherebbero per un file che contiene sicuramente un virus.

  Questa opzione fornisce la scansione più accurata, ma in genere è più lenta di una scansione normale.

- **Ricerca programmi potenzialmente indesiderati**: questa opzione consente di rilevare spyware, adware, dialer e altri programmi di cui non è stata autorizzata l'installazione nel computer.

  NOTA
  Lasciare tutte le opzioni selezionate per effettuare la scansione più accurata possibile. In questo modo vengono analizzati tutti i file presenti nell'unità o nella cartella selezionate, quindi la scansione potrebbe richiedere molto tempo. Maggiori sono la dimensione del disco rigido e il numero di file, maggiore sarà la durata della scansione.

4 Per avviare la scansione dei file, fare clic su **Scansione**.

Al termine della scansione, un riepilogo della scansione mostra il numero di file analizzati, il numero di file rilevati, il numero di programmi potenzialmente indesiderati e il numero di file rilevati che sono stati puliti automaticamente.

5 Fare clic su **OK** per chiudere il riepilogo e visualizzare l'elenco dei file rilevati nella finestra di dialogo **Ricerca virus** (Figura 2-10).

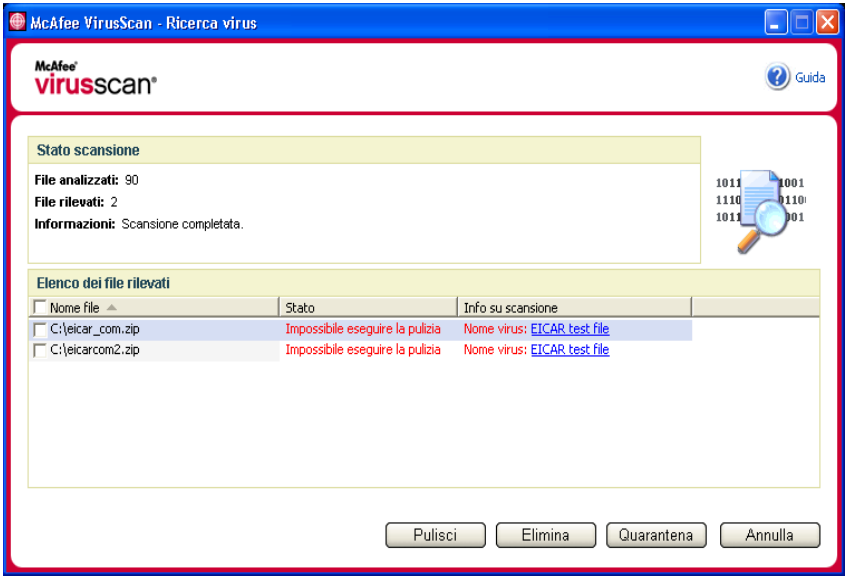


Figura 2-10. Risultati della scansione

NOTA
La scansione conta un file compresso (.ZIP, .CAB e così via) come un file nel numero di **File analizzati**. Inoltre, il numero di file analizzati può variare se si sono eliminati i file temporanei di Internet dopo l'ultima scansione.

6 Se non vengono individuati virus o programmi potenzialmente indesiderati, fare clic su **Indietro** per selezionare un'altra unità o un'altra cartella da analizzare oppure fare clic su **Chiudi** per chiudere la finestra di dialogo. In caso contrario, vedere *Informazioni sul rilevamento delle minacce* a pagina 39.

Scansione tramite Esplora risorse

VirusScan fornisce un menu di scelta rapida per analizzare file, cartelle o unità selezionati ricercando virus e programmi potenzialmente indesiderati da Esplora risorse.

Per analizzare i file in Esplora risorse:

1 Aprire Esplora risorse.

2 Fare clic con il pulsante destro del mouse sull'unità, la cartella o il file da analizzare, quindi scegliere **Ricerca virus**.

Verrà aperta la finestra di dialogo **Ricerca virus** e avrà inizio la scansione dei file. Per impostazione predefinita, tutte le **Opzioni di scansione** predefinite sono preselezionate per offrire la scansione più accurata possibile (Figura 2-8 a pagina 33).

Scansione tramite Microsoft Outlook

VirusScan comprende un'icona della barra degli strumenti per rilevare virus e programmi potenzialmente indesiderati in archivi di messaggi selezionati e rispettive sottocartelle, cartelle delle caselle della posta oppure messaggi di posta elettronica che contengono allegati in Microsoft Outlook 97 o versioni successive.

Per eseguire la scansione della posta elettronica in Microsoft Outlook:

1. Aprire Microsoft Outlook.
2. Fare clic sull'archivio di messaggi, sulla cartella o sul messaggio di posta elettronica che contiene un allegato da analizzare, quindi fare clic sull'icona di scansione della posta nella barra degli strumenti .

   Lo scanner della posta viene aperto e inizia la scansione dei file. Per impostazione predefinita, tutte le **Opzioni di scansione** predefinite sono preselezionate per offrire la scansione più accurata possibile (Figura 2-8 a pagina 33).

Ricerca automatica di virus e altre minacce

Sebbene VirusScan analizzi i file non appena vengono aperti dall'utente o dal computer, è possibile pianificare una scansione automatica nell'Utilità di pianificazione di Windows per cercare accuratamente i virus e i programmi potenzialmente indesiderati a intervalli di tempo specificati.

Per pianificare una scansione:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.

   Verrà visualizzata la finestra di dialogo **Opzioni di VirusScan**.

2 Fare clic sulla scheda **Pianificata** (Figura 2-11 a pagina 38).

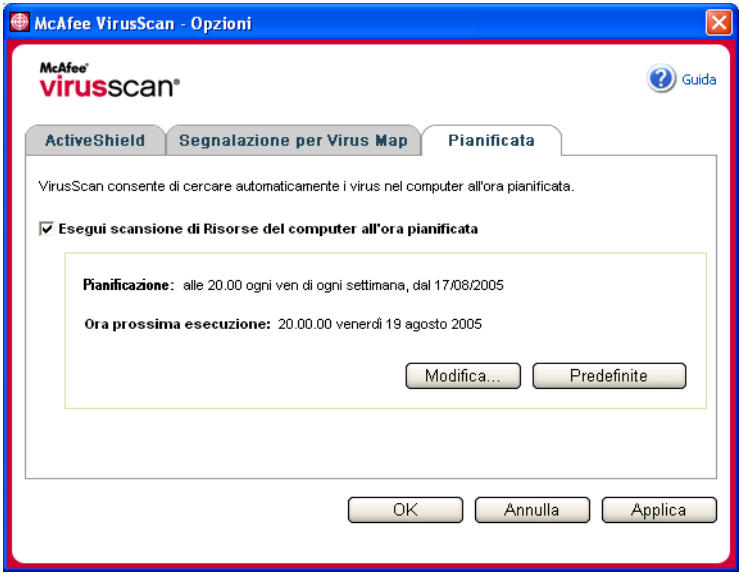


Figura 2-11. Opzioni di scansione pianificata

3 Per attivare la scansione automatica, selezionare la casella di controllo **Esegui scansione di Risorse del computer all'ora pianificata**.

4 Specificare una pianificazione di scansione automatica:

- Per accettare la pianificazione predefinita (alle 20.00 del venerdì di ogni settimana), fare clic su **OK**.
- Per modificare la pianificazione:

  a. Fare clic su **Modifica**.

  b. Selezionare la frequenza di scansione del computer nell'elenco **Pianifica operazione**, quindi selezionare altre opzioni nell'area dinamica sottostante:

  Giornaliera: consente di specificare il numero di giorni tra le scansioni.

  Settimanale (predefinita): consente di specificare il numero di settimane tra le scansioni, nonché i nomi dei giorni della settimana.

  Mensile: consente di specificare il giorno del mese in cui eseguire la scansione. Fare clic su **Seleziona mesi** per specificare i mesi in cui eseguire la scansione, quindi fare clic su **OK**.

Una volta sola: consente di specificare la data in cui eseguire la scansione.

NOTA
Le seguenti opzioni dell'Utilità di pianificazione di Windows non sono supportate:
All'avvio del sistema, **Quando il PC è inattivo** e **Mostra pianificazioni multiple**. Verrà utilizzata l'ultima pianificazione supportata finché non verrà selezionata un'opzione valida.

c. Nella casella **Ora di inizio**, selezionare l'ora del giorno in cui eseguire la scansione.

d. Per selezionare le opzioni avanzate, fare clic su **Avanzate**.

Verrà visualizzata la finestra di dialogo **Opzioni di pianificazione avanzate**.

i. Specificare una data di inizio, una data di fine, la durata, l'ora di fine e se arrestare l'operazione all'ora specificata se la scansione è ancora in esecuzione.

ii. Fare clic su **OK** per salvare le modifiche apportate e chiudere la finestra di dialogo. In alternativa, fare clic su **Annulla**.

5 Fare clic su **OK** per salvare le modifiche apportate e chiudere la finestra di dialogo. In alternativa, fare clic su **Annulla**.

6 Per tornare alla pianificazione predefinita, fare clic su **Predefinite**. In alternativa, fare clic su **OK**.

Informazioni sul rilevamento delle minacce

La funzione di scansione cerca automaticamente di pulire il file per la maggior parte dei virus, cavalli di Troia e worm. È possibile tuttavia scegliere come gestire i file rilevati, nonché decidere se inviarli ai laboratori AVERT di McAfee affinché vengano esaminati. Se la funzione di scansione rileva un programma potenzialmente indesiderato, è possibile provare manualmente a pulirlo, metterlo in quarantena o eliminarlo (l'invio ad AVERT non è disponibile).

Per gestire un virus o un programma potenzialmente indesiderato:

1 Se viene visualizzato un file nell'**Elenco dei file rilevati**, fare clic sulla rispettiva casella di controllo per selezionarlo.

NOTA
Se vengono visualizzati più file nell'elenco, è possibile selezionare la casella di controllo davanti all'elenco **Nome file** per eseguire la stessa operazione su tutti i file. Inoltre, è possibile fare clic sul nome del file nell'elenco **Info su scansione** per visualizzare i dettagli provenienti dalla Libreria di informazioni sui virus.

2 Se il file è un programma potenzialmente indesiderato, è possibile selezionare **Pulisci** per tentare la pulizia del file.

3 Se la funzione di scansione non è in grado di pulire il file, fare clic su **Quarantena** per crittografare e isolare temporaneamente nella directory di quarantena i file infetti o sospetti, fino a quando non sarà possibile effettuare le operazioni appropriate. Per ulteriori informazioni, vedere la sezione *Gestione dei file in quarantena* a pagina 40.

4 Se la funzione di scansione non è in grado di pulire o mettere in quarantena il file, è possibile effettuare una delle seguenti operazioni:

- Fare clic su **Elimina** per rimuovere il file.
- Fare clic su **Annulla** per chiudere la finestra di dialogo senza effettuare altre operazioni.

Se non è possibile pulire o eliminare il file rilevato, consultare la Libreria di informazioni sui virus all'indirizzo http://us.mcafee.com/virusInfo/default.asp per reperire le istruzioni sull'eliminazione manuale dei virus.

Se il file rilevato impedisce l'uso della connessione a Internet o del computer, provare a utilizzare un disco di ripristino per riavviare il sistema. In molti casi è possibile avviare con un disco di ripristino un computer disattivato da un file rilevato. Per ulteriori informazioni, vedere la sezione *Creazione di un disco di ripristino* a pagina 42.

Per ulteriore assistenza, rivolgersi al Servizio clienti McAfee all'indirizzo http://www.mcafeehelp.com/.

Gestione dei file in quarantena

La funzione Quarantena consente di crittografare e isolare temporaneamente nella cartella di quarantena i file infetti e sospetti, fino a quando non sarà possibile effettuare le operazioni appropriate. Dopo la pulizia, i file in quarantena possono essere ripristinati nei percorsi originali.

Per gestire i file in quarantena:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Gestione dei file in quarantena**.

Verrà visualizzato un elenco di file in quarantena (Figura 2-12).

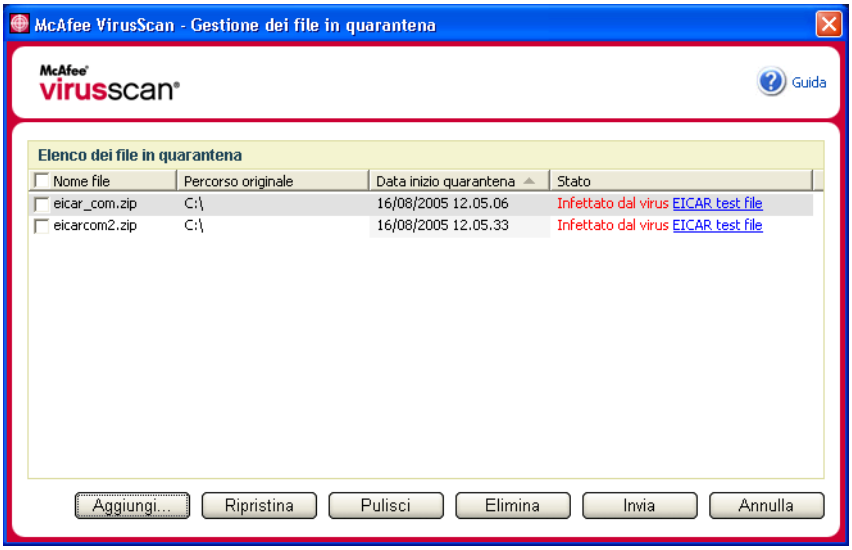


Figura 2-12. Finestra di dialogo Gestione dei file in quarantena

2 Selezionare la casella di controllo accanto al file o ai file da pulire.

> **NOTA**
> Se vengono visualizzati più file nell'elenco, è possibile selezionare la casella di controllo davanti all'elenco **Nome file** per eseguire la stessa operazione su tutti i file. Inoltre, è possibile fare clic sul nome del virus nell'elenco **Stato** per visualizzare i dettagli provenienti dalla Libreria di informazioni sui virus.
>
> In alternativa, fare clic su **Aggiungi**, selezionare un file sospetto da aggiungere all'elenco in quarantena, fare clic su **Apri**, quindi selezionarlo nell'elenco.

3 Fare clic su **Pulisci**.

4 Se il file viene pulito, fare clic su **Ripristina** per riportarlo nel percorso originale.

5 Se VirusScan non è in grado di pulire il virus, fare clic su **Elimina** per rimuovere il file.

6 Se VirusScan non è in grado di pulire o eliminare il file e se non si tratta di un programma potenzialmente indesiderato, è possibile inviarlo all'AntiVirus Emergency Response Team (AVERT™) di McAfee affinché venga esaminato:

   a Aggiornare i file delle firme elettroniche dei virus se risalgono a oltre due settimane prima.

   b Verificare l'abbonamento.

   c Selezionare il file, quindi fare clic su **Invia** per inviare il file ad AVERT.

      VirusScan invia i file in quarantena come allegati in un messaggio di posta elettronica che contiene l'indirizzo di posta elettronica dell'utente, il paese, la versione del software, il sistema operativo e il nome e il percorso originali del file. La dimensione massima di invio è un unico file da 1,5 MB al giorno.

7 Fare clic su **Annulla** per chiudere la finestra di dialogo senza effettuare altre operazioni.

Creazione di un disco di ripristino

Il disco di ripristino è un'utilità che crea un disco floppy avviabile che è possibile utilizzare per avviare il computer ed effettuare la scansione alla ricerca di virus se l'avvio normale è impedito da un virus.

> **NOTA**
> Per scaricare l'immagine del disco di ripristino, è necessario essere connessi a Internet. Il disco di ripristino è disponibile solo per i computer con partizioni FAT (FAT 16 e FAT 32) del disco rigido. Non è necessario per le partizioni NTFS.

Per creare un disco di ripristino:

1 In un computer non infetto, inserire un disco floppy non infetto nell'unità A. Si consiglia di utilizzare la funzione di scansione per assicurarsi che non siano presenti virus nel computer e nel disco floppy. Per ulteriori informazioni, vedere la sezione *Ricerca manuale di virus e altre minacce* a pagina 33.

2 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Crea disco di ripristino**.

Verrà visualizzata la finestra di dialogo **Crea disco di ripristino** (Figura 2-13).

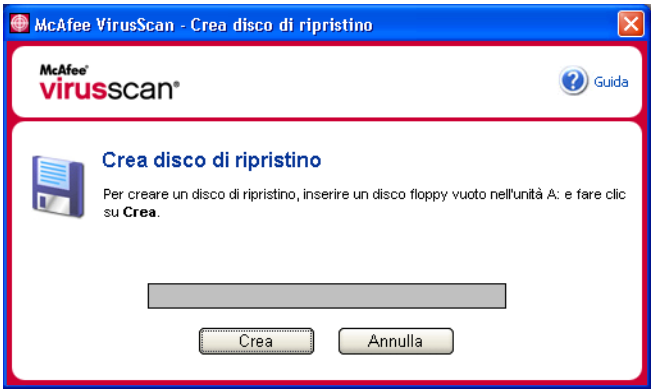

McAfee VirusScan - Crea disco di ripristino
McAfee
virusscan
Guida
Crea disco di ripristino
Per creare un disco di ripristino, inserire un disco floppy vuoto nell'unità A: e fare clic su Crea.
Crea
Annulla

Figura 2-13. Finestra di dialogo Crea disco di ripristino

3 Fare clic su **Crea** per creare il disco di ripristino.

La prima volta che si crea un disco di ripristino viene visualizzato un messaggio in cui si specifica che è necessario scaricare il file immagine per il disco di ripristino. Fare clic su **OK** per scaricare subito il componente oppure su **Annulla** per scaricarlo in un secondo momento.

Viene visualizzato un messaggio di avviso per informare che il contenuto del disco floppy andrà perso.

4 Fare clic su **Sì** per continuare la creazione del disco di ripristino.

Nella finestra di dialogo **Crea disco di ripristino** viene visualizzato lo stato della creazione.

5 Quando viene visualizzato il messaggio "Creazione del disco di ripristino completata", scegliere **OK**, quindi chiudere la finestra di dialogo **Crea disco di ripristino**.

6 Rimuovere il disco di ripristino dall'unità, proteggerlo dalla scrittura e riporlo in un luogo sicuro.

Protezione da scrittura di un disco di ripristino

Per proteggere da scrittura un disco di ripristino:

1 Rivolgere verso il basso il lato con l'etichetta del disco floppy (deve essere visibile il cerchio di metallo).

2 Individuare la linguetta di protezione dalla scrittura. Far scorrere la linguetta in modo che sia visibile il foro.

Utilizzo di un disco di ripristino

Per utilizzare un disco di ripristino:

1. Spegnere il computer infetto.
2. Inserire il disco di ripristino nell'unità.
3. Accendere il computer.

   Verrà visualizzata una finestra grigia con varie opzioni.
4. Scegliere l'opzione che si adatta meglio alle proprie esigenze premendo i rispettivi tasti funzione (ad esempio F2 e F3).

   NOTA
   Se non si preme nessuno di questi tasti entro 60 secondi, verrà avviata automaticamente l'utilità del disco di ripristino.

Aggiornamento di un disco di ripristino

È consigliabile aggiornare regolarmente il disco di ripristino. Per aggiornare il disco di ripristino, attenersi alle istruzioni indicate per la creazione di un disco di ripristino.

Segnalazione automatica dei virus

È possibile inviare in modo anonimo informazioni sui virus da includere nella World Virus Map. È possibile effettuare automaticamente la registrazione per questa funzione gratuita e protetta durante l'installazione di VirusScan (nella finestra di dialogo **Segnalazione per Virus Map**) o in qualsiasi momento nella scheda **Segnalazione per Virus Map** della finestra di dialogo **Opzioni di VirusScan**.

Segnalazione per la World Virus Map

Per segnalare automaticamente le informazioni sui virus alla World Virus Map:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **Opzioni**.

   Verrà visualizzata la finestra di dialogo **Opzioni di VirusScan**.

2 Fare clic sulla scheda **Segnalazione per Virus Map** (Figura 2-14).

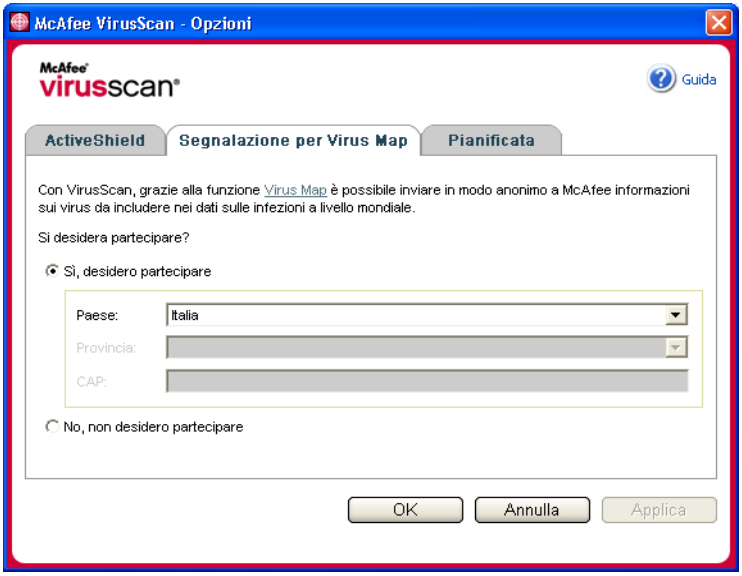


Figura 2-14. Opzioni di Segnalazione per Virus Map

3 Accettare l'opzione predefinita **Sì, desidero partecipare** per inviare in modo anonimo informazioni a McAfee da includere nella World Virus Map delle informazioni sulle infezioni a livello mondiale. In alternativa, selezionare **No, non desidero partecipare** per non inviare le informazioni.

4 Chi risiede negli Stati Uniti, deve selezionare lo stato e immettere il codice postale dell'area in cui si trova il computer. Chi risiede fuori dagli Stati Uniti, deve selezionare il paese in cui si trova il computer.

5 Fare clic su **OK**.

Visualizzazione della World Virus Map

Indipendentemente dalla partecipazione al programma di segnalazione alla World Virus Map, è possibile visualizzare le informazioni più recenti sulle infezioni a livello mondiale facendo clic sull'icona McAfee nella barra delle applicazioni di Windows.

Per visualizzare la World Virus Map:

- Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **VirusScan**, quindi fare clic su **World Virus Map**.

  Verrà visualizzata la pagina Web **World Virus Map** (Figura 2-15).

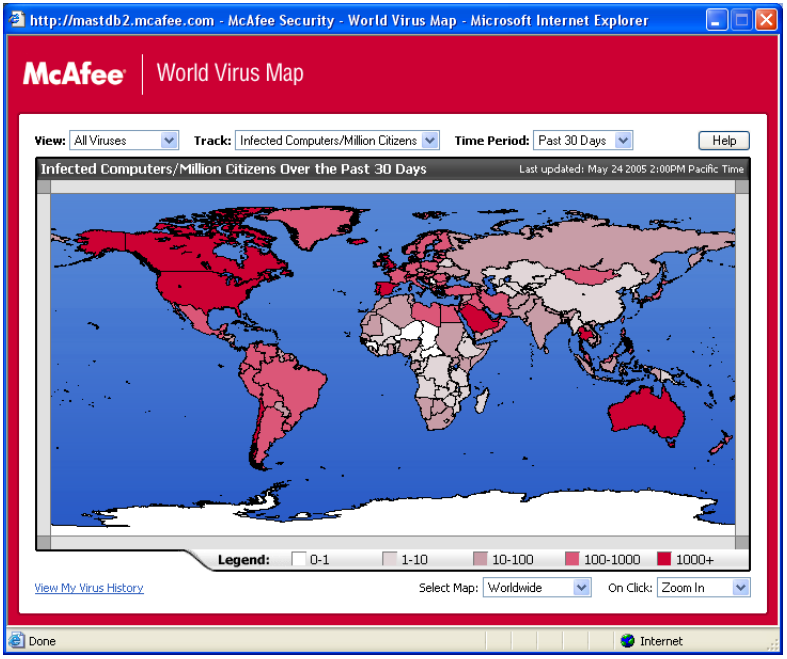

http://mastdb2.mcafee.com - McAfee Security - World Virus Map - Microsoft Internet Explorer
McAfee
World Virus Map
View: All Viruses
Track: Infected Computers/Million Citizens
Time Period: Past 30 Days
Help
Infected Computers/Million Citizens Over the Past 30 Days
Last updated: May 24 2005 2:00PM Pacific Time
Legend: 0-1 1-10 10-100 100-1000 1000+
View My Virus History
Select Map: Worldwide
On Click: Zoom In
Done
Internet

Figura 2-15. World Virus Map

Per impostazione predefinita, la World Virus Map mostra il numero di computer infettati in tutto il mondo negli ultimi 30 giorni e la data di aggiornamento dei dati. È possibile modificare la visualizzazione in modo da mostrare il numero di file infettati oppure è possibile modificare il periodo di tempo per mostrare solo i risultati degli ultimi 7 giorni o delle ultime 24 ore.

Nella sezione **Rintracciamento virus** sono elencati i totali cumulativi dei file analizzati, dei file infetti e dei computer infettati segnalati dalla data indicata.

Aggiornamento di VirusScan

Quando si è connessi a Internet, VirusScan verifica automaticamente la disponibilità di aggiornamenti ogni quattro ore, quindi scarica e installa automaticamente gli aggiornamenti settimanali delle firme elettroniche dei virus (file .dat) senza interrompere le operazioni in corso.

I file .dat hanno una dimensione di circa 100 KB , quindi hanno un impatto minimo sulle prestazioni del sistema durante il download.

In caso di disponibilità di un aggiornamento di un prodotto o di epidemia di virus, verrà visualizzato un avviso. Una volta avvisati, sarà possibile scegliere di aggiornare VirusScan per eliminare la minaccia di un'epidemia di virus.

Verifica automatica degli aggiornamenti

McAfee SecurityCenter è configurato automaticamente per verificare gli aggiornamenti di tutti i servizi McAfee ogni quattro ore quando si è connessi a Internet e per notificare tali aggiornamenti con avvisi e segnali acustici. Per impostazione predefinita, SecurityCenter scarica e installa automaticamente tutti gli aggiornamenti disponibili.

NOTA
In alcuni casi, verrà richiesto di riavviare il computer per completare l'aggiornamento. Prima di riavviare, assicurarsi di salvare tutti i dati e chiudere tutte le applicazioni.

Verifica manuale degli aggiornamenti

Oltre alla verifica automatica ogni quattro ore durante la connessione a Internet, è possibile verificare manualmente la disponibilità di aggiornamenti in qualsiasi momento.

Per verificare manualmente la disponibilità di aggiornamenti di VirusScan:

1. Assicurarsi che il computer sia connesso a Internet.
2. Fare clic con il pulsante destro del mouse sull'icona McAfee, quindi scegliere **Aggiornamenti**.

   Verrà visualizzata la finestra di dialogo **Aggiornamenti di SecurityCenter**.
3. Fare clic su **Controlla**.

   Se è disponibile un aggiornamento, verrà visualizzata la finestra di dialogo **Aggiornamenti di VirusScan** (Figura 2-16 a pagina 48). Fare clic su **Aggiorna** per continuare.

Se non è disponibile alcun aggiornamento, verrà visualizzata una finestra di dialogo per segnalare che VirusScan è aggiornato. Fare clic su **OK** per chiudere la finestra di dialogo.

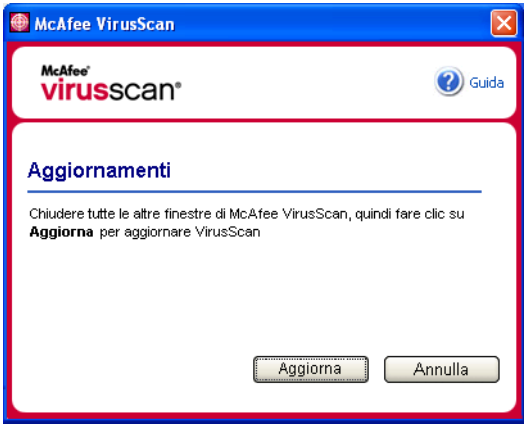


Figura 2-16. Finestra di dialogo Aggiornamenti

4 Se richiesto, accedere al sito Web. La **procedura guidata di aggiornamento** consente di installare automaticamente l'aggiornamento.

5 Al termine dell'installazione dell'aggiornamento fare clic su **Fine**.

NOTA
In alcuni casi, verrà richiesto di riavviare il computer per completare l'aggiornamento. Prima di riavviare, assicurarsi di salvare tutti i dati e chiudere tutte le applicazioni.

McAfee Personal Firewall Plus 3

Benvenuti in McAfee Personal Firewall Plus.

Il software McAfee Personal Firewall Plus offre una protezione avanzata per il computer e per i dati personali. Personal Firewall consente di stabilire una barriera tra il computer in uso e Internet, monitorando il traffico Internet alla ricerca di attività sospette, senza richiedere interazione da parte dell'utente.

Grazie a questo software, è possibile usufruire delle seguenti funzioni:

- Difende dagli attacchi degli hacker
- Completa la difesa antivirus
- Controlla Internet e le attività della rete
- Segnala eventi potenzialmente dannosi
- Fornisce informazioni dettagliate sul traffico Internet sospetto
- Integra la funzionalità Hackerwatch.org, che include la creazione di rapporti sugli eventi, gli strumenti di test e la possibilità di inviare tramite posta elettronica gli eventi rilevati ad altre autorità online
- Fornisce funzioni dettagliate di ricerca e traccia degli eventi

Nuove funzioni

- **Supporto per i giochi potenziato**
  McAfee Personal Firewall Plus protegge il computer dai tentativi di intrusione e dalle attività sospette durante l'esecuzione di giochi a schermo intero, ma può nascondere gli avvisi se rileva tentativi di intrusione o attività sospette. Gli avvisi rossi vengono visualizzati dopo aver chiuso il gioco.

- **Gestione dell'accesso a Internet potenziata**
  McAfee Personal Firewall Plus consente agli utenti di concedere in modo dinamico alle applicazioni l'accesso temporaneo a Internet. L'accesso è limitato all'intervallo che intercorre tra quando viene avviata l'applicazione e quando viene chiusa. Se Personal Firewall rileva un programma sconosciuto che sta tentando di comunicare con Internet, un avviso rosso offre l'opzione di concedere all'applicazione l'accesso temporaneo a Internet.

- **Controllo della protezione potenziato**
  Se si esegue la funzione di blocco, McAfee Personal Firewall Plus consente di bloccare immediatamente tutto il traffico Internet in ingresso e in uscita tra il computer e Internet. Gli utenti possono attivare e disattivare il blocco direttamente da queste tre posizioni in Personal Firewall.

- **Opzioni di recupero potenziate**
  È possibile eseguire le Opzioni di ripristino per ripristinare automaticamente le impostazioni predefinite in Personal Firewall. Se Personal Firewall mostra un comportamento diverso da quello previsto, che non è possibile correggere, è possibile annullare le impostazioni correnti e tornare alle impostazioni predefinite del programma.

- **Protezione della connettività Internet**
  Per evitare che un utente disattivi inavvertitamente la connessione Internet, se Personal Firewall rileva una connessione Internet originata da un server DHCP o DNS, l'opzione di esclusione di un indirizzo Internet non viene inclusa negli avvisi blu. L'opzione viene visualizzata se il traffico in ingresso non viene originato da un server DHCP o DNS.

- **Integrazione con HackerWatch.org potenziata**
  La segnalazione di potenziali hacker è più facile che mai. McAfee Personal Firewall Plus migliora la funzionalità di HackerWatch.org, che comprende l'invio di eventi potenzialmente dannosi al database.

- **Gestione intelligente delle applicazioni estesa**
  Quando un'applicazione tenta di accedere a Internet, Personal Firewall verifica se è affidabile o dannosa. Se viene riconosciuta come affidabile, Personal Firewall ne consente automaticamente l'accesso a Internet, senza che sia necessario l'intervento dell'utente.

- **Rilevamento avanzato dei cavalli di Troia**
  McAfee Personal Firewall Plus combina la gestione delle connessioni delle applicazioni con un database potenziato per rilevare e bloccare l'accesso a Internet e la possibile ritrasmissione di dati personali da parte di più applicazioni potenzialmente dannose, come i cavalli di Troia.

- **Miglioramento di Visual Trace**
  Visual Trace comprende mappe grafiche intuitive che illustrano l'origine degli attacchi ostili e il traffico a livello mondiale, incluse informazioni dettagliate sul contatto/proprietario, a partire dagli indirizzi IP di origine.

- **Maggiore facilità d'uso**
  McAfee Personal Firewall Plus comprende un Assistente di installazione e un'Esercitazione per gli utenti che facilitano l'installazione e l'uso del firewall. Il prodotto è stato progettato per essere utilizzato senza alcun intervento, tuttavia McAfee offre una vasta gamma di risorse che permettono di capire e apprezzare le capacità del firewall.

- **Rilevamento delle intrusioni potenziato**
  Il Sistema di rilevamento intrusioni (IDS) di Personal Firewall rileva i più comuni tipi di attacco e altre attività sospette. Il rilevamento delle intrusioni controlla la presenza di trasferimenti di dati o metodi di trasferimento sospetti in ogni pacchetto di dati e li inserisce nel registro degli eventi.

- **Analisi del traffico potenziata**
  McAfee Personal Firewall Plus offre agli utenti una visualizzazione dei dati in ingresso e in uscita dei computer, nonché una visualizzazione delle connessioni delle applicazioni, comprese quelle di connessioni aperte che sono attivamente "in ascolto". In questo modo gli utenti possono vedere quali sono le applicazioni aperte a un'eventuale intrusione e intervenire di conseguenza.

Rimozione di altri firewall

Prima di installare il software McAfee Personal Firewall Plus, è necessario rimuovere eventuali altri programmi firewall presenti sul computer. Seguire le istruzioni di disinstallazione del programma firewall.

NOTA
Se si utilizza Windows XP, non è necessario disattivare il firewall incorporato prima di installare McAfee Personal Firewall Plus. Tuttavia, si consiglia di farlo. In caso contrario, non si riceveranno gli eventi nel registro Eventi in ingresso di McAfee Personal Firewall Plus.

Impostazione del firewall predefinito

McAfee Personal Firewall è in grado di gestire le autorizzazioni e il traffico per le applicazioni Internet presenti sul computer anche se Windows Firewall è in esecuzione.

Una volta installato, McAfee Personal Firewall disattiva automaticamente Windows Firewall e viene impostato come firewall predefinito. È quindi possibile utilizzare solo le funzionalità e i messaggi di McAfee Personal Firewall. Se in seguito si attiva Windows Firewall mediante Windows Security Center o il Pannello di controllo di Windows, l'esecuzione di entrambi i firewall sul computer potrebbe causare una parziale perdita di registrazione in McAfee Firewall, nonché la duplicazione di messaggi di stato e di avviso.

NOTA
Se entrambi i firewall sono attivati, nella scheda Eventi in ingresso di McAfee Personal Firewall non vengono visualizzati tutti gli indirizzi IP bloccati. Windows Firewall intercetta e blocca la maggior parte di questi eventi, impedendo a McAfee Personal Firewall di rilevarli o registrarli. McAfee Personal Firewall potrebbe tuttavia bloccare e registrare ulteriore traffico in base ad altri fattori di sicurezza.

In Windows Firewall la registrazione è disattivata per impostazione predefinita, ma se si attivano entrambi i firewall è possibile attivare tale registrazione. Il percorso del registro di Windows Firewall predefinito è C:\Windows\pfirewall.log.

Per garantire che il computer sia protetto da almeno un firewall, Windows Firewall viene automaticamente riattivato quando si disinstalla McAfee Personal Firewall.

Se si disattiva McAfee Personal Firewall o si imposta il livello di protezione su **Aperto** senza attivare manualmente Windows Firewall, l'intera protezione del firewall viene rimossa a eccezione delle applicazioni bloccate in precedenza.

Impostazione del livello di protezione

È possibile configurare le opzioni di protezione per indicare la modalità di risposta di Personal Firewall quando viene rilevato traffico indesiderato. Per impostazione predefinita, è attivato il livello di protezione **Standard**. Con il livello di protezione **Standard**, quando si consente a un'applicazione l'accesso a Internet, viene consentito l'accesso completo. L'accesso completo consente all'applicazione di inviare e ricevere dati non richiesti su porte non di sistema.

Per configurare le impostazioni di protezione:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Opzioni**.
2. Fare clic sull'icona **Impostazioni di protezione**.
3. Impostare il livello di protezione desiderato utilizzando il dispositivo di scorrimento.

   La gamma di livelli di protezione va da Blocco ad Aperto:

   - **Blocco:** tutte le connessioni a Internet sul computer vengono chiuse. È possibile utilizzare questa impostazione per bloccare porte configurate per essere aperte nella pagina Servizi di sistema.
   - **Protezione elevata:** se un'applicazione richiede solo un tipo di accesso a Internet specifico (ad esempio Solo accesso in uscita), è possibile concedere o meno una connessione Internet all'applicazione. Se in seguito l'applicazione richiede l'accesso completo, è possibile concederlo o mantenere solo l'accesso in uscita.
   - **Standard (impostazione consigliata):** se un'applicazione richiede l'accesso a Internet e questo le viene concesso, viene consentito l'accesso completo per gestire il traffico in ingresso e in uscita.

- **Protezione basata sull'affidabilità:** tutte le applicazioni vengono automaticamente ritenute affidabili al primo tentativo di accesso a Internet. È tuttavia possibile configurare Personal Firewall in modo da poter utilizzare gli avvisi per la notifica di nuove applicazioni sul computer. Utilizzare questa impostazione in caso di mancato funzionamento di alcuni giochi o dello streaming audio o video.

- **Aperto:** il firewall è disattivato. Questa impostazione consente il passaggio di tutto il traffico attraverso Personal Firewall senza alcun filtro.

  NOTA
  Quando il livello di protezione del firewall è impostato su **Aperto** o **Blocco**, le applicazioni bloccate in precedenza continuano a essere bloccate. Per impedire che ciò si verifichi, è possibile impostare le autorizzazioni dell'applicazione su **Accesso completo** oppure eliminare la regola di autorizzazione **Blocco** nell'elenco **Applicazioni Internet**.

4 Selezionare ulteriori impostazioni di protezione:

  NOTA
  Se si utilizza Windows XP e sono stati aggiunti più utenti di XP, le opzioni riportate di seguito sono disponibili solo se si accede al computer in qualità di amministratore.

- **Registra eventi di Sistema di rilevamento intrusioni (IDS) nel registro Eventi in ingresso:** se si seleziona questa opzione, gli eventi rilevati da IDS vengono visualizzati nel registro Eventi in ingresso. Il Sistema di rilevamento delle intrusioni rileva i tipi di attacco comuni e altre attività sospette. Il rilevamento delle intrusioni verifica tutti i pacchetti di dati in ingresso e in uscita alla ricerca di trasferimenti di dati o metodi di trasferimento sospetti, li confronta con un database di firme ed esclude automaticamente quelli provenienti dal computer che genera l'attacco.

  IDS cerca specifici modelli di traffico utilizzati dagli hacker. IDS verifica tutti i pacchetti ricevuti dal computer alla ricerca di traffico sospetto o attacchi noti. Ad esempio, se in Personal Firewall vengono visualizzati i pacchetti ICMP, tali pacchetti vengono analizzati alla ricerca di modelli di traffico sospetti confrontando il traffico ICMP con modelli di attacco noti.

- **Accetta richieste ping ICMP:** il traffico ICMP viene utilizzato principalmente per l'esecuzione di tracce e ping. Il ping viene spesso utilizzato per eseguire una rapida verifica prima di tentare di stabilire le comunicazioni. Se si utilizza o si è utilizzato un programma di condivisione di file peer-to-peer, è possibile che si riceva un numero elevato di ping. Se si seleziona questa opzione, Personal Firewall consente tutte le richieste di ping senza registrare i ping nel registro Eventi in ingresso. Se l'opzione non è selezionata, Personal Firewall blocca tutte le richieste di ping e registra i ping nel registro Eventi in ingresso.

- **Consenti a utenti con restrizioni di modificare impostazioni di Personal Firewall:** se si utilizza Windows XP o Windows 2000 Professional con più utenti, selezionare questa opzione per consentire agli utenti XP con restrizioni di modificare le impostazioni di Personal Firewall.

5 Dopo aver apportato le modifiche desiderate, fare clic su **OK**.

Verifica di McAfee® Personal Firewall Plus

È possibile verificare l'installazione di Personal Firewall per controllarne la possibile vulnerabilità a intrusioni e attività sospette.

Per verificare l'installazione di Personal Firewall dall'icona McAfee visualizzata nella barra delle applicazioni:

- Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows e selezionare **Prova firewall**.

Viene avviato Internet Explorer e viene visualizzato il sito Web di HackerWatch gestito da McAfee all'indirizzo http://www.hackerwatch.org/. Per verificare Personal Firewall, seguire le istruzioni visualizzate nella pagina Probe di Hackerwatch.org.

Informazioni sulla pagina Riepilogo

Il riepilogo di Personal Firewall comprende quattro pagine riassuntive:

- Riepilogo principale
- Riepilogo applicazione
- Riepilogo eventi
- Riepilogo di HackerWatch

Le pagine Riepilogo contengono una grande varietà di rapporti sugli eventi recenti in ingresso, sullo stato delle applicazioni e sulle attività di intrusione in tutto il mondo segnalate da HackerWatch.org, nonché collegamenti alle operazioni più comuni eseguite in Personal Firewall.

Per aprire la pagina Riepilogo principale in Personal Firewall:

- Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Visualizza riepilogo** (Figura 3-1).

McAfee® Personal Firewall Plus
File Modifica Visualizza Evento ?
personalfirewallplus
Blocca
Impostazioni
Guida
Riepilogo principale (Modifica visualizzazione)
Riepilogo
Applicazioni Internet
Eventi in ingresso
Opzioni
Il firewall è impostato su Protezione standard.
324 nuovi eventi sono stati bloccati oggi.
39 regole per applicazioni sono state sostituite di recente.
Novità
Ultimo aggiornamento: 24/08/2005 16.30.19
L'applicazione GMT ha ottenuto l'accesso completo a Internet. Può pertanto comunicare con Internet.
Visualizza ulteriori informazioni
Ultimo evento
Ultimo aggiornamento: 24/08/2005 16.26.23
Un computer con Indirizzo IP 10.2.39.111 ha tentato di accedere a una delle porte del sistema (TCP porta 139).
Rintraccia evento
Considera affidabile questo indirizzo IP
Rapporto giornaliero
Rapporto giornaliero del numero totale di eventi in ingresso bloccati.
Oggi 324
Questa settimana 324
Questo mese 324
Applicazioni attive
Elenco delle applicazioni in esecuzione nel computer.
Processo di sistema
Attività comuni
Visualizza traffico Internet corrente
Modifica impost. firewall
Visualizza guida in linea
Protezione standard
Indirizzo IP: 10.2.36.86 Maschera di rete: 255.255.252.0

Figura 3-1. Pagina Riepilogo principale

Fare clic sulle seguenti opzioni per accedere alle varie pagine Riepilogo:

Voce	Descrizione
Modifica visualizzazione	Fare clic su **Modifica visualizzazione** per aprire un elenco di pagine Riepilogo. Nell'elenco selezionare una pagina Riepilogo da visualizzare.
Freccia destra	Fare clic sull'icona a forma di freccia rivolta verso destra per visualizzare la pagina Riepilogo successiva.
Freccia sinistra	Fare clic sull'icona a forma di freccia rivolta verso sinistra per visualizzare la pagina Riepilogo precedente.
Home Page	Fare clic sull'icona della home page per tornare alla pagina **Riepilogo principale**.

Nella pagina Riepilogo principale sono disponibili le seguenti informazioni:

Voce	Descrizione
Impostazione di protezione	Lo stato dell'impostazione di protezione indica il livello di protezione su cui è impostato il firewall. Fare clic sul collegamento per modificare il livello di protezione.
Eventi bloccati	Lo stato eventi bloccati visualizza il numero di eventi bloccati nel corso della giornata. Fare clic sul collegamento per visualizzarne i dettagli provenienti dalla pagina Eventi in ingresso.
Modifiche regole applicazioni	Lo stato della regola dell'applicazione visualizza il numero di regole applicazioni che sono state modificate di recente. Fare clic sul collegamento per visualizzare l'elenco di applicazioni consentite e bloccate nonché per modificare le autorizzazioni delle applicazioni.
Novità	**Novità** visualizza l'ultima applicazione a cui è stato consentito l'accesso completo a Internet.
Ultimo evento	**Ultimo evento** visualizza gli eventi in ingresso più recenti. È possibile fare clic su un collegamento per rintracciare l'evento o per impostare l'indirizzo IP come affidabile. Se si imposta un indirizzo IP come affidabile, si consente a tutto il traffico che ne proviene di raggiungere il computer.
Rapporto giornaliero	**Rapporto giornaliero** visualizza il numero di eventi in ingresso bloccati da Personal Firewall durante la giornata, la settimana e il mese in corso. Fare clic sul collegamento per visualizzarne i dettagli provenienti dalla pagina Eventi in ingresso.
Applicazioni attive	**Applicazioni attive** visualizza le applicazioni attualmente in esecuzione nel computer e connesse a Internet. Fare clic su un'applicazione per visualizzare gli indirizzi IP a cui l'applicazione è connessa.
Attività comuni	Fare clic su un collegamento nell'area **Attività comuni** per andare alle pagine di Personal Firewall in cui è possibile visualizzare l'attività del firewall ed eseguire le attività.

Per visualizzare la pagina Riepilogo applicazione:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Visualizza riepilogo**.
2. Fare clic su **Modifica visualizzazione**, quindi selezionare **Riepilogo applicazione**.

Nella pagina Riepilogo applicazione sono disponibili le seguenti informazioni:

Voce	Descrizione
Controllo traffico	**Controllo traffico** visualizza le connessioni Internet in ingresso e in uscita nel corso degli ultimi quindici minuti. Fare clic sul grafico per visualizzare i dettagli di controllo del traffico.
Applicazioni attive	**Applicazioni attive** visualizza l'utilizzo della larghezza di banda delle applicazioni più attive del computer nel corso delle ultime 24 ore. **Applicazione**: l'applicazione che accede a Internet. **%**: la percentuale di larghezza di banda utilizzata dall'applicazione. **Autorizzazione**: il tipo di accesso a Internet consentito all'applicazione. **Regola creata**: data e ora di creazione della regola per l'applicazione.
Novità	**Novità** visualizza l'ultima applicazione a cui è stato consentito l'accesso completo a Internet.
Applicazioni attive	**Applicazioni attive** visualizza le applicazioni attualmente in esecuzione nel computer e connesse a Internet. Fare clic su un'applicazione per visualizzare gli indirizzi IP a cui l'applicazione è connessa.
Attività comuni	Fare clic su un collegamento nell'area **Attività comuni** per andare alle pagine di Personal Firewall in cui è possibile vedere lo stato dell'applicazione ed eseguire attività relative all'applicazione.

Per visualizzare la pagina Riepilogo eventi:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Visualizza riepilogo**.
2. Fare clic su **Modifica visualizzazione**, quindi selezionare **Riepilogo eventi**.

Nella pagina Riepilogo eventi sono disponibili le seguenti informazioni:

Voce	Descrizione
Confronto porte	**Confronto porte** visualizza un grafico a torta relativo alle porte del computer in uso su cui è stato effettuato il maggior numero di tentativi nel corso degli ultimi 30 giorni. È possibile fare clic sul nome di una porta per visualizzarne i dettagli provenienti dalla pagina Eventi in ingresso. È inoltre possibile spostare il puntatore del mouse sul numero di una porta per visualizzarne una descrizione.
Principali eventi	**Principali eventi** visualizza gli indirizzi IP bloccati più di frequente, la data e l'ora in cui si è verificato l'ultimo evento in ingresso per ogni indirizzo e il numero totale di eventi in ingresso nel corso degli ultimi trenta giorni per ogni indirizzo. Fare clic su un evento per visualizzarne i dettagli provenienti dalla pagina Eventi in ingresso.
Rapporto giornaliero	**Rapporto giornaliero** visualizza il numero di eventi in ingresso bloccati da Personal Firewall durante la giornata, la settimana e il mese in corso. Fare clic su un numero per visualizzare i dettagli dell'evento provenienti dalla pagina Eventi in ingresso.
Ultimo evento	**Ultimo evento** visualizza gli eventi in ingresso più recenti. È possibile fare clic su un collegamento per rintracciare l'evento o per impostare l'indirizzo IP come affidabile. Se si imposta un indirizzo IP come affidabile, si consente a tutto il traffico che ne proviene di raggiungere il computer.
Attività comuni	Fare clic su un collegamento nell'area **Attività comuni** per accedere alle pagine di Personal Firewall in cui è possibile visualizzare i dettagli degli eventi ed eseguire attività relative agli eventi.

Per visualizzare la pagina Riepilogo di HackerWatch:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Visualizza riepilogo**.
2. Fare clic su **Modifica visualizzazione**, quindi selezionare **Riepilogo di HackerWatch**.

Nella pagina Riepilogo di HackerWatch sono disponibili le informazioni seguenti.

Voce	Descrizione
Attività a livello mondiale	**Attività a livello mondiale** visualizza una mappa mondiale in cui sono identificate le attività bloccate di recente controllate da HackerWatch.org. Fare clic sulla mappa per aprire la mappa di Analisi delle minacce globali in HackerWatch.org.
Traccia degli eventi	**Traccia degli eventi** visualizza il numero di eventi in ingresso inviati a HackerWatch.org.
Attività globale delle porte	**Attività globale delle porte** visualizza le porte principali che sono state minacciate nel corso degli ultimi cinque giorni. Fare clic su una porta per visualizzarne il numero e la descrizione.
Attività comuni	Fare clic su un collegamento nell'area **Attività comuni** per accedere alle pagine di HackerWatch.org in cui è possibile ottenere ulteriori informazioni sulle attività degli hacker in tutto il mondo.

Informazioni sulla pagina Applicazioni Internet

Nella pagina Applicazioni Internet viene visualizzato l'elenco delle applicazioni autorizzate e bloccate.

Per avviare la pagina Applicazioni Internet:

- Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Applicazioni Internet** (Figura 3-2).

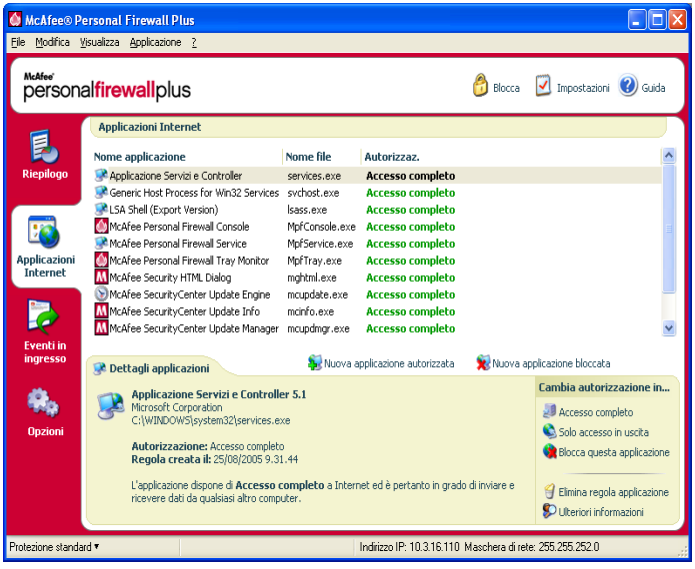


Figura 3-2. Pagina Applicazioni Internet

Nella pagina Applicazioni Internet sono disponibili le seguenti informazioni:

- Nomi delle applicazioni
- Nomi dei file
- Livelli di autorizzazione correnti
- Dettagli sulle applicazioni: nome e versione dell'applicazione, nome della società, nome del percorso, timestamp e spiegazione dei tipi di autorizzazione

Modifica delle regole delle applicazioni

Personal Firewall consente di modificare le regole di accesso per le applicazioni.

Per modificare la regola di un'applicazione:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **Personal Firewall**, quindi selezionare **Applicazioni Internet**.
2. Nell'elenco **Applicazioni Internet**, fare clic con il pulsante destro del mouse sulla regola di un'applicazione e selezionare un livello diverso:
   - **Accesso completo:** consente all'applicazione di stabilire connessioni Internet in uscita e in ingresso.
   - **Solo accesso in uscita:** consente all'applicazione di stabilire solo una connessione Internet in uscita.
   - **Blocca questa applicazione:** non consente all'applicazione di accedere a Internet.

     NOTA
     Quando il livello di protezione del firewall è impostato su **Aperto** o **Blocco**, le applicazioni bloccate in precedenza continuano a essere bloccate. Per impedire che ciò si verifichi, è possibile impostare la regola di accesso dell'applicazione su **Accesso completo** oppure eliminare la regola di autorizzazione **Blocco** dall'elenco **Applicazioni Internet**.

Per eliminare la regola di un'applicazione:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Applicazioni Internet**.
2. Nell'elenco **Applicazioni Internet**, fare clic con il pulsante destro del mouse sulla regola dell'applicazione, quindi selezionare **Eliminare regola applicazione**.

Alla successiva richiesta di accesso a Internet da parte dell'applicazione, sarà possibile impostarne il livello di autorizzazione per aggiungerla nuovamente all'elenco.

Autorizzazione e blocco delle applicazioni Internet

Per modificare l'elenco delle applicazioni Internet autorizzate e bloccate:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Applicazioni Internet**.
2. Nella pagina Applicazioni Internet, fare clic su una delle seguenti opzioni:
   - **Nuova applicazione autorizzata:** consente all'applicazione l'accesso completo a Internet.
   - **Nuova applicazione bloccata:** non consente all'applicazione di accedere a Internet.
   - **Elimina regola applicazione:** consente di rimuovere la regola di un'applicazione.

Informazioni sulla pagina Eventi in ingresso

Utilizzare la pagina Eventi in ingresso per visualizzare il registro Eventi in ingresso generato quando le connessioni Internet non richieste vengono bloccate da Personal Firewall.

Per aprire la pagina Eventi in ingresso:

- Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso** (Figura 3-3).

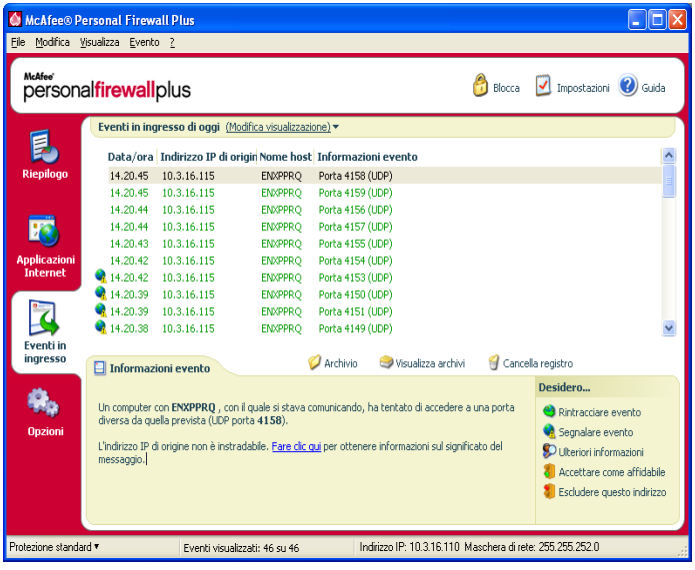

McAfee® Personal Firewall Plus
File Modifica Visualizza Evento ?
personalfirewallplus
Blocca
Impostazioni
Guida
Riepilogo
Applicazioni Internet
Eventi in ingresso
Opzioni
Eventi in ingresso di oggi (Modifica visualizzazione)
Data/ora Indirizzo IP di origin Nome host Informazioni evento
14.20.45 10.3.16.115 ENXPPRQ Porta 4158 (UDP)
14.20.45 10.3.16.115 ENXPPRQ Porta 4159 (UDP)
14.20.44 10.3.16.115 ENXPPRQ Porta 4156 (UDP)
14.20.44 10.3.16.115 ENXPPRQ Porta 4157 (UDP)
14.20.43 10.3.16.115 ENXPPRQ Porta 4155 (UDP)
14.20.42 10.3.16.115 ENXPPRQ Porta 4154 (UDP)
14.20.42 10.3.16.115 ENXPPRQ Porta 4153 (UDP)
14.20.39 10.3.16.115 ENXPPRQ Porta 4150 (UDP)
14.20.39 10.3.16.115 ENXPPRQ Porta 4151 (UDP)
14.20.38 10.3.16.115 ENXPPRQ Porta 4149 (UDP)
Informazioni evento
Archivio
Visualizza archivi
Cancella registro
Un computer con ENXPPRQ , con il quale si stava comunicando, ha tentato di accedere a una porta diversa da quella prevista (UDP porta 4158).
L'indirizzo IP di origine non è instradabile. Fare clic qui per ottenere informazioni sul significato del messaggio.
Desidero...
Rintracciare evento
Segnalare evento
Ulteriori informazioni
Accettare come affidabile
Escludere questo indirizzo
Protezione standard
Eventi visualizzati: 46 su 46
Indirizzo IP: 10.3.16.110 Maschera di rete: 255.255.252.0

Figura 3-3. Pagina Eventi in ingresso

Nella pagina Eventi in ingresso sono disponibili le seguenti informazioni:

- Timestamp
- Indirizzi IP di origine
- Nomi host
- Nomi del servizio o dell'applicazione
- Dettagli eventi: tipi di connessione, porte di connessione, nome host o IP e spiegazione del significato degli eventi relativi alle varie porte

Informazioni sugli eventi

Informazioni sugli indirizzi IP

Gli indirizzi IP sono numeri. Per la precisione, sono costituiti da quattro numeri compresi tra 0 e 255. Tali numeri indicano una destinazione precisa a cui può essere indirizzato il traffico su Internet.

I tipi di indirizzi IP

Numerosi indirizzi IP sono considerati speciali per varie ragioni:

Indirizzi IP non instradabili: detti anche "spazi IP privati". Questi indirizzi IP non possono essere utilizzati in Internet. I blocchi privati sono 10.x.x.x, 172.16.x.x - 172.31.x.x e 192.168.x.x.

Indirizzi IP di loop-back: gli indirizzi di loop-back vengono utilizzati a scopo di test. Il traffico inviato a questo blocco di indirizzi IP torna subito al dispositivo che genera il pacchetto, non lascia mai il dispositivo e viene utilizzato principalmente per test di hardware e software. Il blocco di indirizzi IP di loop-back è 127.x.x.x.

Indirizzo IP nullo: indirizzo non valido. Una volta rilevato, Personal Firewall indica che il traffico utilizzava un indirizzo IP vuoto. Spesso questa situazione indica che l'origine del traffico viene deliberatamente nascosta dal mittente. Il mittente non sarà in grado di ricevere risposte al traffico, a meno che il pacchetto non venga ricevuto da un'applicazione in grado di comprendere i contenuti del pacchetto in cui sono incluse istruzioni specifiche per tale applicazione. Qualsiasi indirizzo che inizi per 0 (0.x.x.x) è un indirizzo nullo. Ad esempio, 0.0.0.0 è un indirizzo IP nullo.

Eventi da 0.0.0.0

Due sono le cause più probabili per il rilevamento di eventi dall'indirizzo IP 0.0.0.0. La prima causa, più comune, è che il computer abbia ricevuto un pacchetto non corretto. Internet non è sempre affidabile al 100% ed è possibile che vengano inoltrati pacchetti non validi. Poiché i pacchetti vengono esaminati da Personal Firewall prima della convalida da parte di TCP/IP, è possibile che vengano segnalati come evento.

Nel secondo caso, l'indirizzo IP di origine ha subito un attacco di tipo spoofing, ovvero è stato contraffatto. I pacchetti contraffatti possono indicare la scansione in corso del computer alla ricerca di cavalli di Troia. Personal Firewall blocca questo tipo di attività, quindi il computer in uso è sicuro.

Eventi da 127.0.0.1

Alcuni eventi vengono generati dall'indirizzo IP 127.0.0.1. Questo viene chiamato indirizzo di loopback o localhost.

Molti programmi legittimi utilizzano infatti l'indirizzo di loopback per la comunicazione fra i componenti. Ad esempio, è possibile configurare molti server di posta elettronica o Web tramite un'interfaccia Web. Per accedere all'interfaccia, digitare “http://localhost/” nel browser Web.

Il traffico proveniente da tali programmi viene autorizzato da Personal Firewall, quindi se si rilevano eventi da 127.0.0.1, è probabile che l'indirizzo IP di origine sia stato sottoposto a spoofing, ovvero sia stato contraffatto. I pacchetti contraffatti indicano in genere che un altro computer sta eseguendo la scansione del proprio computer alla ricerca di cavalli di Troia. Personal Firewall blocca questi tentativi di intrusione, quindi il computer in uso è sicuro.

Esistono programmi, come Netscape 6.2 e versioni successive, che richiedono l'aggiunta di 127.0.0.1 all'elenco degli indirizzi IP affidabili. La modalità di comunicazione tra i componenti di tali programmi non consente a Personal Firewall di determinare se si tratti o meno di traffico locale.

Nel caso di Netscape 6.2, se non si imposta 127.0.0.1 come affidabile, non sarà possibile utilizzare l'elenco degli amici. Se si rileva quindi traffico proveniente da 127.0.0.1 e tutte le applicazioni del computer funzionano normalmente, è possibile bloccare tale traffico senza che si verifichino problemi. Se tuttavia in un programma, ad esempio Netscape, si verificano problemi, aggiungere 127.0.0.1 all'elenco Indirizzi IP affidabili di Personal Firewall, quindi verificare se i problemi sono stati risolti.

Se l'inserimento di 127.0.0.1 nell'elenco degli indirizzi IP affidabili consente di risolvere il problema, è necessario valutare attentamente le opzioni disponibili. Se si imposta 127.0.0.1 come affidabile, il programma funzionerà correttamente, ma il sistema sarà più vulnerabile ad attacchi di spoofing. Se non si ritiene affidabile l'indirizzo, il programma non funzionerà correttamente, ma il sistema sarà protetto dal traffico dannoso.

Eventi dai computer nella LAN

Gli eventi possono essere generati dai computer presenti nella LAN. Questi eventi vengono visualizzati in verde, a indicare che provengono dalla rete.

Nella maggior parte delle configurazioni LAN aziendali si consiglia di selezionare la casella di controllo **Considera affidabili tutti i computer della LAN** nella finestra di dialogo Indirizzi IP affidabili.

In determinate situazioni, la rete "locale" può essere tanto pericolosa quanto Internet, soprattutto se si utilizza una rete DSL o con modem via cavo a larghezza di banda elevata. In questo caso, non selezionare **Considera affidabili tutti i computer della LAN**. Aggiungere invece gli indirizzi IP dei computer locali all'elenco degli indirizzi IP affidabili.

Eventi dagli indirizzi IP privati

Gli indirizzi IP con formato 192.168.xxx.xxx, 10.xxx.xxx.xxx e 172.16.0.0 - 172.31.255.255 sono detti non instradabili o privati. Tali indirizzi IP non dovrebbero mai lasciare la rete e possono essere considerati quasi sempre affidabili.

Il blocco 192.168 xxx.xxx viene utilizzato con Condivisione connessione Internet di Microsoft (ICS). Se si utilizza Condivisione connessione Internet e si rilevano eventi provenienti da tale blocco IP, è possibile aggiungere l'indirizzo IP 192.168.255.255 all'elenco degli indirizzi IP affidabili. In tal modo verrà impostato come affidabile l'intero blocco 192.168.xxx.xxx.

Se non si è connessi a una rete privata e si rilevano eventi provenienti da tali intervalli IP, è possibile che gli indirizzi IP di origine siano stati sottoposti a spoofing, ovvero siano stati contraffatti. I pacchetti contraffatti indicano in genere una scansione per la ricerca di cavalli di Troia. È importante ricordare che tale tentativo è stato bloccato da Personal Firewall, quindi il computer in uso è sicuro.

Poiché gli indirizzi IP privati fanno riferimento a computer diversi a seconda della rete a cui si è connessi, la segnalazione di tali eventi risulta inutile, quindi non viene effettuata.

Visualizzazione degli eventi nel registro Eventi in ingresso

Nel registro Eventi in ingresso, gli eventi vengono visualizzati in numerosi modi diversi. La visualizzazione predefinita mostra solo gli eventi che si verificano nel corso della giornata. È possibile visualizzare anche gli eventi che si sono verificati durante la settimana scorsa oppure il registro completo.

Grazie a Personal Firewall è inoltre possibile visualizzare eventi in ingresso relativi a giorni specifici, provenienti da specifici indirizzi Internet (indirizzi IP) o contenenti le stesse informazioni sull'evento.

Per informazioni su un evento, fare clic sull'evento. Le informazioni verranno visualizzate nel riquadro **Informazioni evento**.

Visualizzazione degli eventi odierni

Utilizzare questa opzione per rivedere gli eventi odierni.

Per visualizzare gli eventi odierni:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse su una voce, quindi fare clic su **Mostra eventi di oggi**.

Visualizzazione degli eventi della settimana

Utilizzare questa opzione per rivedere gli eventi settimanali.

Per visualizzare gli eventi della settimana:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse su una voce, quindi fare clic su **Mostra eventi di questa settimana**.

Visualizzazione del registro Eventi in ingresso completo

Utilizzare questa opzione per rivedere tutti gli eventi.

Per visualizzare tutti gli eventi nel registro Eventi in ingresso:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **Personal Firewall**, quindi fare clic su **Eventi in ingresso**.
2. Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse su una voce, quindi fare clic su **Mostra registro completo**.

   Il registro degli eventi in ingresso visualizza tutti gli eventi del registro.

Visualizzazione degli eventi di un giorno specifico

Utilizzare questa opzione per rivedere gli eventi di un giorno specifico.

Per visualizzare gli eventi di un giorno specifico:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse su una voce, quindi fare clic su **Mostra solo eventi del giorno selezionato**.

Visualizzazione degli eventi da un indirizzo Internet specifico

Utilizzare questa opzione per rivedere gli eventi che vengono originati da un particolare indirizzo Internet.

Per visualizzare gli eventi di un indirizzo Internet:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall** e fare clic su **Eventi in ingresso**.
2. Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse su una voce, quindi fare clic su **Mostra solo eventi dell'indirizzo Internet selezionato**.

Visualizzazione di eventi con le stesse informazioni sull'evento

Utilizzare questa opzione per rivedere gli eventi nel registro degli eventi in ingresso per i quali nella colonna Informazioni evento sono riportate le stesse informazioni dell'evento selezionato. È possibile verificare quante volte si è verificato l'evento e se proviene dalla stessa origine. La colonna Informazioni evento contiene una descrizione dell'evento e, se noto, il programma o il servizio comune che utilizza la porta interessata.

Per visualizzare gli eventi con le stesse informazioni sull'evento:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall** e fare clic su **Eventi in ingresso**.
2. Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse su una voce, quindi fare clic su **Mostra solo eventi con le stesse informazioni sull'evento**.

Risposta agli eventi in ingresso

Oltre a rivedere informazioni dettagliate sugli eventi visualizzati nel registro Eventi in ingresso, è possibile creare con Visual Trace una traccia degli indirizzi IP di un evento del registro Eventi in ingresso oppure ottenere informazioni sull'evento visitando HackerWatch.org, il sito Web della comunità online per la protezione dagli attacchi degli hacker.

Traccia dell'evento selezionato

È possibile tentare di creare con Visual Trace una traccia visuale degli indirizzi IP relativi a un evento riportato nel registro Eventi in ingresso.

Per creare la traccia di un evento selezionato:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall** e selezionare **Eventi in ingresso**.

2 Nel registro degli eventi in ingresso, fare clic con il pulsante destro del mouse sull'evento per il quale si desidera creare una traccia, quindi fare clic su **Rintraccia evento selezionato**. Per creare la traccia di un evento, è possibile anche fare doppio clic sull'evento.

Per impostazione predefinita, la traccia visuale viene avviata in Personal Firewall mediante il programma Visual Trace di Personal Firewall.

Suggerimenti da HackerWatch.org

Per ottenere suggerimenti da HackerWatch.org:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **Personal Firewall** e selezionare **Eventi in ingresso**.

2 Selezionare l'evento nella pagina Eventi in ingresso, quindi fare clic su **Ulteriori informazioni** nel riquadro **Desidero**.

Il browser Web predefinito verrà aperto e verrà visualizzato il sito Web HackerWatch.org in cui sono disponibili informazioni relative al tipo di evento e suggerimenti relativi all'opportunità di segnalare l'evento.

Segnalazione di un evento

Per segnalare un evento che si ritiene essere un attacco al computer in uso:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall** e selezionare **Eventi in ingresso**.

2 Fare clic sull'evento che si desidera segnalare, quindi fare clic su **Segnalare evento** nel riquadro **Desidero**.

Personal Firewall segnala l'evento al sito Web HackerWatch.org, utilizzando l'ID univoco del computer in uso.

Registrazione a HackerWatch.org

Alla prima apertura della pagina Riepilogo, HackerWatch.org verrà contattato da Personal Firewall per generare un ID utente univoco. Se si è già utenti registrati, la richiesta di accesso verrà convalidata automaticamente. Ai nuovi utenti viene richiesta l'immissione di uno pseudonimo e di un indirizzo di posta elettronica. Per utilizzare le funzionalità di filtro e di invio tramite posta elettronica degli eventi disponibili nel sito Web sarà quindi necessario fare clic sul collegamento di convalida disponibile nel messaggio di posta elettronica di conferma di HackerWatch.org.

È possibile segnalare l'evento al sito Web HackerWatch.org senza convalidare l'ID utente. Tuttavia, per filtrare gli eventi e inviare un messaggio di posta elettronica a un amico, è necessario abbonarsi al servizio.

L'abbonamento a tale servizio consente di tenere traccia delle segnalazioni inviate e di ricevere avvisi, nel caso in cui a HackerWatch.org siano necessarie più informazioni o ulteriori azioni da parte dell'utente. L'abbonamento consente inoltre di verificare tutte le informazioni ricevute, in modo da poterle utilizzare.

Tutti gli indirizzi di posta elettronica forniti a HackerWatch.org rimangono riservati. Se una richiesta di ulteriori informazioni viene inviata da un ISP, tale richiesta viene reindirizzata tramite HackerWatch.org, in modo da non esporre mai l'indirizzo di posta elettronica degli utenti.

Considerazione di un indirizzo come affidabile

È possibile utilizzare la pagina Eventi in ingresso per aggiungere un indirizzo IP all'elenco degli indirizzi IP affidabili e consentire una connessione permanente.

Se nella pagina Eventi in ingresso viene individuato un evento contenente un indirizzo IP che si desidera autorizzare, è possibile impostare Personal Firewall in modo che le connessioni da tale indirizzo siano consentite in qualunque momento.

Per aggiungere un indirizzo IP all'elenco degli indirizzi IP affidabili:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall** e selezionare **Eventi in ingresso**.
2. Fare clic con il pulsante destro del mouse sull'evento contenente l'indirizzo IP da impostare come affidabile e scegliere **Considera affidabile l'indirizzo IP di origine**.

Verificare che l'indirizzo IP visualizzato nel messaggio di conferma Accettare come affidabile sia corretto, quindi fare clic su **OK**. L'indirizzo IP viene aggiunto all'elenco.

Per assicurarsi che l'indirizzo IP sia stato aggiunto:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall** e selezionare **Opzioni**.
2. Fare clic sull'icona **IP affidabili ed esclusi**, quindi sulla scheda **Indirizzi IP affidabili**.

L'indirizzo IP verrà visualizzato come attivato nell'elenco degli indirizzi IP affidabili.

Esclusione di un indirizzo

La visualizzazione di un indirizzo IP nel registro Eventi in ingresso indica che il traffico proveniente da tale indirizzo è stato bloccato. Pertanto, l'esclusione di un indirizzo non aggiunge ulteriore protezione a meno che il computer non abbia porte deliberatamente aperte dalla funzione Servizi di sistema o un'applicazione autorizzata a ricevere dati.

Aggiungere un indirizzo IP all'elenco di esclusione solo se si dispone di una o più porte deliberatamente aperte e se si ha motivo di credere che sia necessario bloccarle.

Se nella pagina Eventi in ingresso viene individuato un evento contenente un indirizzo IP che si desidera escludere, è possibile configurare Personal Firewall in modo che le connessioni da tale indirizzo non siano mai consentite.

È possibile utilizzare la pagina Eventi in ingresso, che elenca gli indirizzi IP del traffico Internet in ingresso, per escludere un indirizzo IP che sembra essere l'origine di attività Internet sospette o indesiderate.

Per aggiungere un indirizzo IP all'elenco degli indirizzi IP esclusi:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. La pagina Eventi in ingresso elenca gli indirizzi IP del traffico Internet in ingresso. Selezionare un indirizzo IP, quindi eseguire una delle seguenti operazioni:
   - Fare clic con il pulsante destro del mouse sull'indirizzo IP, quindi selezionare **Escludi l'indirizzo IP di origine**.
   - Fare clic su **Escludere questo indirizzo** nel menu **Desidero**.
3. Nella finestra di dialogo Aggiungi regola indirizzi IP esclusi, utilizzare una o più impostazioni seguenti per configurare la regola dell'indirizzo IP escluso:
   - **Indirizzo IP singolo:** l'indirizzo IP da escludere. L'indirizzo predefinito è quello selezionato nella pagina Eventi in ingresso.
   - **Intervallo di indirizzi IP:** gli indirizzi IP tra l'indirizzo specificato in Da indirizzo IP e l'indirizzo specificato in A indirizzo IP.
   - **Data scadenza regola:** data e ora in cui la regola dell'indirizzo IP escluso scade. Per selezionare la data e l'ora, selezionare i menu a discesa appropriati.
   - **Descrizione:** se lo si desidera, descrivere la nuova regola.
   - Fare clic su **OK**.
4. Nella finestra di dialogo, fare clic su **Sì** per confermare l'impostazione. Fare clic su **No** per tornare alla finestra di dialogo Aggiungi regola indirizzi IP esclusi.

Se viene rilevato un evento proveniente da una connessione Internet esclusa, verrà inviato un avviso in base al metodo specificato nella pagina Impostazioni avviso.

Per assicurarsi che l'indirizzo IP sia stato aggiunto:

1. Fare clic sulla scheda **Opzioni**.
2. Fare clic sull'icona **IP affidabili ed esclusi**, quindi sulla scheda **Indirizzi IP esclusi**.

L'indirizzo IP verrà visualizzato come attivato nell'elenco degli indirizzi IP esclusi.

Gestione del registro Eventi in ingresso

È possibile utilizzare la pagina Eventi in ingresso per gestire gli eventi del registro Eventi in ingresso generati quando il traffico Internet non richiesto viene bloccato da Personal Firewall.

Archiviazione del registro Eventi in ingresso

È possibile archiviare il registro degli eventi in ingresso corrente per salvare tutti gli eventi in ingresso registrati, incluse la data e le ore, gli IP di origine, i nomi di host, le porte e le informazioni sull'evento. Il registro degli eventi in ingresso va archiviato periodicamente per evitare che diventi troppo grande.

Per archiviare il registro Eventi in ingresso:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. Nella pagina Eventi in ingresso, fare clic su **Archivio**.
3. Nella finestra di dialogo Archivia registro, fare clic su **Sì** per procedere con l'operazione.
4. Fare clic su **Salva** per salvare l'archivio nel percorso predefinito oppure scegliere un percorso in cui salvare l'archivio.

Nota: per impostazione predefinita, Personal Firewall archivia automaticamente il registro degli eventi in ingresso. Selezionare o deselezionare **Archivia automaticamente gli eventi registrati** nella pagina Impostazioni registro eventi per attivare o disattivare l'opzione.

Visualizzazione dei registri Eventi in ingresso archiviati

È possibile visualizzare i registri Eventi in ingresso archiviati in precedenza. L'archivio salvato include la data e le ore, gli IP di origine, i nomi host, le porte e le informazioni sugli eventi.

Per visualizzare il registro degli eventi in ingresso archiviato:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. Nella pagina Eventi in ingresso, fare clic su **Visualizza archivi**.
3. Selezionare o cercare il nome file dell'archivio e fare clic su **Apri**.

Cancellazione del registro Eventi in ingresso

È possibile cancellare tutte le informazioni dal registro Eventi in ingresso.

ATTENZIONE: una volta cancellato il registro Eventi in ingresso, non sarà possibile recuperarne il contenuto. Se si ritiene di averne bisogno in futuro, si consiglia di archiviare il Registro eventi anziché cancellarlo.

Per cancellare il registro Eventi in ingresso:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. Nella pagina Eventi in ingresso, fare clic su **Cancella registro**.
3. Fare clic su **Sì** nella finestra di dialogo per cancellare il registro.

Copia di un evento negli Appunti

È possibile copiare un evento negli Appunti per incollarlo in un file di testo utilizzando il Blocco note.

Per copiare gli eventi negli appunti:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.
2. Fare clic con il pulsante destro del mouse sull'evento nel registro degli eventi in ingresso.
3. Fare clic su **Copia negli Appunti evento selezionato**.
4. Avviare Blocco note.
   - Digitare `notepad` nella riga di commando oppure fare clic su **Start**, scegliere **Programmi**, quindi **Accessori**. Selezionare **Blocco note**.

5 Fare clic su **Modifica**, quindi su Incolla. Il testo dell'evento verrà visualizzato nel Blocco note. Ripetere il passaggio fino a quando non saranno disponibili tutti gli eventi necessari.

6 Salvare il file del Blocco note in un percorso protetto.

Eliminazione dell'evento selezionato

È possibile eliminare eventi dal registro Eventi in ingresso.

Per eliminare eventi dal registro Eventi in ingresso:

1 Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **Personal Firewall**, quindi selezionare **Eventi in ingresso**.

2 Nella pagina Eventi in ingresso, fare clic sull'evento che si desidera eliminare.

3 Nel menu Modifica, fare clic su **Elimina evento selezionato**. L'evento viene eliminato dal registro degli eventi in ingresso.

Informazioni sugli avvisi

Si consiglia di acquisire familiarità con i tipi di avviso che verranno visualizzati durante l'utilizzo di Personal Firewall. Esaminare i seguenti tipi di avviso che possono essere visualizzati e le possibili risposte, in modo da poter reagire con sicurezza.

NOTA
I suggerimenti sugli avvisi aiutano a deciderne la gestione. Per visualizzare i suggerimenti sugli avvisi, fare clic sulla scheda **Opzioni**, sull'icona **Impostazioni avviso**, quindi selezionare **Usa suggerimenti intelligenti** (opzione predefinita) o **Visualizza solo suggerimenti intelligenti** dall'elenco **Suggerimenti intelligenti**.

Avvisi rossi

Gli avvisi rossi contengono informazioni importanti che richiedono l'attenzione immediata dell'utente:

- **Applicazione Internet bloccata:** questo avviso viene visualizzato se Personal Firewall blocca l'accesso a Internet di un'applicazione. Ad esempio, se viene visualizzato un avviso relativo a un programma cavallo di Troia, a tale programma viene automaticamente impedito l'accesso a Internet e all'utente viene consigliato di cercare i virus nel computer.

- **L'applicazione richiede l'accesso a Internet:** questo avviso viene visualizzato quando Personal Firewall rileva traffico Internet o di rete per le nuove applicazioni.

- **L'applicazione è stata modificata:** questo avviso viene visualizzato quando Personal Firewall rileva una modifica a un'applicazione a cui in precedenza era stato consentito l'accesso a Internet. Se l'applicazione non è stata aggiornata di recente, si consiglia di non concedere facilmente l'accesso a Internet all'applicazione modificata.
- **L'applicazione richiede l'Accesso server:** questo avviso viene visualizzato quando Personal Firewall rileva che un'applicazione a cui in precedenza era stato consentito l'accesso a Internet ha richiesto l'accesso a Internet come server.

NOTA
L'impostazione predefinita Aggiornamenti automatici di Windows XP SP2 scarica e installa gli aggiornamenti per il sistema operativo Windows e per gli altri programmi Microsoft eseguiti sul computer senza segnarlo agli utenti. Quando un'applicazione viene modificata da uno degli aggiornamenti invisibili di Windows, gli avvisi di McAfee Personal Firewall vengono visualizzati al successivo avvio dell'applicazione Microsoft.

IMPORTANTE
È necessario consentire l'accesso alle applicazioni che richiedono l'accesso a Internet per scaricare gli ultimi aggiornamenti del prodotto online, quali i servizi di McAfee.

Avviso Applicazione Internet bloccata

Se viene visualizzato un avviso relativo a un programma cavallo di Troia (Figura 3-4), Personal Firewall impedisce automaticamente a tale programma l'accesso a Internet e all'utente viene consigliato di cercare i virus nel computer. Se non è installato McAfee VirusScan, è possibile avviare McAfee SecurityCenter.

McAfee Personal Firewall Plus
Applicazione Internet bloccata.
L'applicazione tt.exe è stata riconosciuta come cavallo di Troia. L'accesso a Internet per tale applicazione è stato automaticamente revocato.
Percorso: C:\Programmi\Trojans\tt.exe
McAfee suggerisce di
Eseguire una scansione per cercare virus nel computer.
Desidero...
Visualizzare registro applicazioni
Avviare McAfee Security Center
Continuare l'operazione in corso

Figura 3-4. Avviso Applicazione Internet bloccata

Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Ulteriori informazioni** per ottenere informazioni dettagliate sull'evento consultando il registro Eventi in ingresso (per ulteriori informazioni vedere *Informazioni sulla pagina Eventi in ingresso* a pagina 61).
- Fare clic su **Avvia McAfee VirusScan** per cercare i virus nel computer.
- Fare clic su **Continuare l'operazione in corso** se non si desidera effettuare altre operazioni, oltre a quelle eseguite da Personal Firewall.
- Fare clic su **Consenti accesso in uscita** per consentire una connessione in uscita (protezione **Elevata**).

Avviso L'applicazione richiede l'accesso a Internet

Se si seleziona **Standard** o **Elevata** nelle opzioni delle impostazioni di protezione, viene visualizzato un avviso (Figura 3-5) quando vengono rilevate connessioni Internet o di rete per le applicazioni nuove o modificate.

McAfee Personal Firewall Plus
L'applicazione richiede l'accesso a Internet
Il programma Firefox ha richiesto l'accesso a Internet. Concedere l'accesso?
Percorso: C:\Programmi\Mozilla Firefox\firefox.exe
Desidero...
Consentire accesso
Consenti accesso una volta sola
Bloccare tutti gli accessi
Guida alla scelta

Figura 3-5. Avviso L'applicazione richiede l'accesso a Internet

Se viene visualizzato un avviso in cui viene raccomandata attenzione nel consentire l'accesso dell'applicazione a Internet, è possibile fare clic su **Per ulteriori informazioni, fare clic qui** per ottenere ulteriori informazioni sull'applicazione. Questa opzione viene visualizzata nell'avviso solo se Personal Firewall è configurato per utilizzare i suggerimenti intelligenti.

McAfee potrebbe non riconoscere l'applicazione durante il tentativo di accesso a Internet (Figura 3-6).

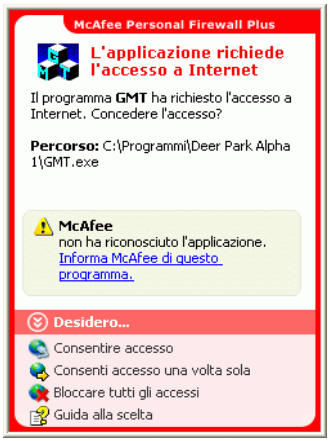

McAfee Personal Firewall Plus
L'applicazione richiede l'accesso a Internet
Il programma GMT ha richiesto l'accesso a Internet. Concedere l'accesso?
Percorso: C:\Programmi\Deer Park Alpha 1\GMT.exe
McAfee
non ha riconosciuto l'applicazione.
Informa McAfee di questo programma.
Desidero...
Consentire accesso
Consenti accesso una volta sola
Bloccare tutti gli accessi
Guida alla scelta

Figura 3-6. Avviso Applicazione non riconosciuta

Pertanto, potrebbe non fornire indicazioni su come gestirla. È possibile segnalare l'applicazione a McAfee facendo clic su **Informa McAfee di questo programma**. Viene visualizzata una pagina Web che chiede le informazioni relative all'applicazione. Inserire il maggior numero di informazioni disponibili.

Le informazioni inviate dagli utenti vengono utilizzate, in combinazione con altri strumenti di ricerca, dai nostri operatori HackerWatch per determinare se un'applicazione deve essere inserita nel nostro database di applicazioni note e, in tal caso, come deve essere gestita da Personal Firewall.

Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Consenti accesso** per consentire all'applicazione di stabilire una connessione Internet in uscita e in ingresso.
- Fare clic su **Consenti accesso una volta sola** per concedere all'applicazione una connessione Internet temporanea. L'accesso è limitato all'intervallo che intercorre tra quando viene avviata l'applicazione e quando viene chiusa.
- Fare clic su **Blocca tutti gli accessi** per impedire la connessione Internet.
- Fare clic su **Consenti accesso in uscita** per consentire una connessione in uscita (protezione **Elevata**).
- Fare clic su **Guida alla scelta** per visualizzare la Guida in linea sulle autorizzazioni di accesso delle applicazioni.

Avviso L'applicazione è stata modificata

Se è stata selezionata la protezione **Basata sull'affidabilità**, **Standard** o **Elevata** nelle opzioni di impostazione di protezione, viene visualizzato un avviso (Figura 3-7) quando Personal Firewall rileva una modifica in un'applicazione che in precedenza era stata autorizzata ad accedere a Internet. Se l'applicazione in questione non è stata aggiornata di recente, si consiglia di non concedere facilmente l'accesso a Internet all'applicazione modificata.

McAfee Personal Firewall Plus
L'applicazione è stata modificata.
L'applicazione Windows Media Player è stata modificata dopo l'autorizzazione all'accesso a Internet. Consentire comunque l'accesso a Internet?
Percorso: C:\Programmi\Windows Media Player\wmplayer.exe
Desidero...
Consentire accesso
Consenti accesso una volta sola
Bloccare tutti gli accessi
Guida alla scelta

Figura 3-7. Avviso L'applicazione è stata modificata

Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Consenti accesso** per consentire all'applicazione di stabilire una connessione Internet in uscita e in ingresso.
- Fare clic su **Consenti accesso una volta sola** per concedere all'applicazione una connessione Internet temporanea. L'accesso è limitato all'intervallo che intercorre tra quando viene avviata l'applicazione e quando viene chiusa.
- Fare clic su **Blocca tutti gli accessi** per impedire la connessione Internet.
- Fare clic su **Consenti accesso in uscita** per consentire una connessione in uscita (protezione **Elevata**).
- Fare clic su **Guida alla scelta** per visualizzare la Guida in linea sulle autorizzazioni di accesso delle applicazioni.

Avviso L'applicazione richiede l'Accesso server

Se è stata selezionata la protezione **Elevata** nelle opzioni di impostazione di protezione, viene visualizzato un avviso (Figura 3-8) quando Personal Firewall rileva che un'applicazione, che in precedenza era stata autorizzata ad accedere a Internet, ha richiesto l'accesso a Internet come server.

McAfee Personal Firewall Plus
L'applicazione richiede l'Accesso server
L'applicazione iTunes ha richiesto di funzionare come server e accettare le connessioni in ingresso. Concedere l'Accesso server?
Percorso: C:\Programmi\iTunes \iTunes.exe
Desidero...
Consenti accesso una volta sola
Consentire accesso server
Consentire solo accesso in uscita
Bloccare tutti gli accessi
Guida alla scelta

Figura 3-8. Avviso L'applicazione richiede l'Accesso server

Ad esempio, un avviso viene visualizzato quando MSN Messenger richiede accesso al server per inviare un file durante una conversazione.

Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Consenti accesso una volta sola** per consentire all'applicazione un accesso a Internet temporaneo. L'accesso è limitato all'intervallo che intercorre tra quando viene avviata l'applicazione e quando viene chiusa.
- Fare clic su **Consenti accesso server** per consentire all'applicazione di stabilire una connessione Internet in uscita e in ingresso.
- Fare clic su **Consenti solo accesso in uscita** per impedire le connessioni Internet in ingresso.
- Fare clic su **Blocca tutti gli accessi** per impedire la connessione Internet.
- Fare clic su **Guida alla scelta** per visualizzare la Guida in linea sulle autorizzazioni di accesso delle applicazioni. Avvisi verdi

Avvisi verdi

Gli avvisi verdi indicano la presenza di eventi in Personal Firewall, come le applicazioni a cui è stato automaticamente concesso l'accesso a Internet.

Programma autorizzato all'accesso a Internet: questo avviso viene visualizzato quando l'accesso a Internet viene concesso automaticamente a tutte le applicazioni nuove e viene emessa una notifica (protezione **Basata sull'affidabilità**). Un esempio di applicazione modificata è un'applicazione con regole modificate per consentirne automaticamente l'accesso a Internet.

Avviso Programma autorizzato all'accesso a Internet

Se nelle opzioni di impostazione di protezione è stata selezionata la protezione **Basata sull'affidabilità**, Personal Firewall consente automaticamente l'accesso a Internet a tutte le applicazioni nuove, quindi informa l'utente con un avviso (Figura 3-9).

McAfee Personal Firewall Plus
Programma autorizzato all'accesso a Internet
Il programma Windows Messenger è stato automaticamente autorizzato all'accesso a Internet.
Percorso: C:\Programmi\Messenger\msmsgs.exe
Applicazione autorizzata.
McAfee ha riconosciuto l'applicazione.
Per ulteriori informazioni, fare clic qui.
Desidero...
Visualizzare registro applicazioni
Disattivare tipo di avviso
Continuare l'operazione in corso

Figura 3-9. Programma autorizzato all'accesso a Internet

Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Visualizzare registro applicazioni** per ottenere informazioni dettagliate sull'evento mediante il registro Eventi in ingresso applicazioni Internet (per ulteriori informazioni vedere *Informazioni sulla pagina Applicazioni Internet* a pagina 59).
- Per evitare la visualizzazione di questi tipi di avvisi, fare clic su **Disattivare tipo di avviso**.
- Fare clic su **Continuare l'operazione in corso** se non si desidera effettuare altre operazioni, oltre a quelle eseguite da Personal Firewall.
- Fare clic su **Blocca tutti gli accessi** per impedire la connessione Internet.

Avviso L'applicazione è stata modificata

Se nelle opzioni di impostazione di protezione è stata selezionata la protezione **Basata sull'affidabilità**, Personal Firewall consente automaticamente l'accesso a Internet a tutte le applicazioni modificate. Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Visualizzare registro applicazioni** per ottenere informazioni dettagliate sull'evento mediante il registro Eventi in ingresso applicazioni Internet (per ulteriori informazioni vedere *Informazioni sulla pagina Applicazioni Internet* a pagina 59).
- Per evitare la visualizzazione di questi tipi di avvisi, fare clic su **Disattivare tipo di avviso**.
- Fare clic su **Continuare l'operazione in corso** se non si desidera effettuare altre operazioni, oltre a quelle eseguite da Personal Firewall.
- Fare clic su **Blocca tutti gli accessi** per impedire la connessione Internet.

Avvisi blu

Gli avvisi blu contengono informazioni, ma non richiedono una reazione da parte dell'utente.

- **Tentativo di connessione bloccato:** questo avviso viene visualizzato quando il traffico Internet o di rete indesiderato viene bloccato da Personal Firewall (Protezione basata su affidabilità, standard o elevata).

Avviso Tentativo di connessione bloccato

Se è stata seleziona la protezione **Basata sull'affidabilità**, **Standard** o **Elevata**, viene visualizzato un avviso (Figura 3-10) in caso di blocco del traffico Internet o di rete indesiderato.

McAfee Personal Firewall Plus
Tentativo di connessione bloccato
Un computer con Indirizzo IP 10.3.16.115, con il quale si stava comunicando, ha tentato di accedere a una porta diversa da quella prevista (UDP porta 1482).
Desidero...
Visualizzare registro eventi
Rintracciare questo indirizzo
Disattivare tipo di avviso
Continuare l'operazione in corso

Figura 3-10. Avviso Tentativo di connessione bloccato

Visualizzare una breve descrizione dell'evento, quindi scegliere una delle seguenti opzioni:

- Fare clic su **Visualizzare registro eventi** per ottenere informazioni dettagliate sull'evento mediante il registro Eventi in ingresso di Personal Firewall (per ulteriori informazioni vedere *Informazioni sulla pagina Eventi in ingresso* a pagina 61).
- Fare clic su **Rintracciare questo indirizzo** per creare una traccia visuale degli indirizzi IP relativi all'evento.
- Fare clic su **Escludere questo indirizzo** per bloccare l'accesso al computer di questo indirizzo. L'indirizzo verrà aggiunto all'elenco degli indirizzi IP esclusi.
- Fare clic su **Accettare come affidabile** per consentire l'accesso di questo indirizzo IP al computer.
- Fare clic su **Continuare l'operazione in corso** se non si desidera effettuare altre operazioni, oltre a quelle eseguite da Personal Firewall.

McAfee Privacy Service 4

Benvenuti in McAfee Privacy Service.

Il software McAfee Privacy Service offre una protezione avanzata per utenti privati, famiglie, dati personali e computer.

Funzioni

In questa versione di McAfee Privacy Service sono disponibili le seguenti funzioni:

- Regole per gli orari di utilizzo di Internet: attraverso una griglia è possibile specificare i giorni e gli orari durante i quali gli utenti possono accedere a Internet.
- Filtro personalizzato mediante parole chiave: consente di filtrare l'accesso ai siti Web in base a parole chiave specificate dall'amministratore per i diversi gruppi di età.
- Backup e ripristino di Privacy Service: consente di salvare e ripristinare le impostazioni di Privacy Service in qualsiasi momento.
- Blocco di Web bug: consente di bloccare i Web bug (oggetti scaricati da siti Web potenzialmente pericolosi) in modo che non vengano caricati nelle pagine Web visitate.
- Blocco di popup: consente di impedire la visualizzazione delle finestre popup durante la navigazione in Internet.
- Shredder: McAfee Shredder protegge la privacy grazie alla cancellazione rapida e sicura dei file indesiderati.

L'amministratore

L'amministratore specifica quali utenti possono accedere a Internet, in quali orari e quali operazioni possono effettuare online.

NOTA
L'amministratore è considerato un adulto e in quanto tale può accedere a tutti i siti Web nonché consentire o impedire la trasmissione di informazioni di identificazione personale (PII).

Assistente di installazione

Assistente di installazione consente di creare l'amministratore (se l'operazione non è già stata eseguita), di gestire le impostazioni generali, di immettere informazioni personali e di aggiungere utenti.

NOTA

Per poter effettuare l'accesso a Privacy Service è necessario ricordare la password di amministratore e la risposta di sicurezza. Senza aver effettuato l'accesso, non è possibile utilizzare Privacy Service e Internet. Mantenere segreta la password per non consentire ad altri di modificare le impostazioni di Privacy Service.

Alcuni siti Web richiedono l'attivazione dei cookie per poter funzionare correttamente.

Privacy Service accetta sempre i cookie di McAfee.com.

Recupero della password di amministratore

Se si dimentica la password di amministratore, è possibile recuperarla utilizzando le informazioni di sicurezza immesse al momento della creazione del profilo dell'amministratore.

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows, scegliere **McAfee Privacy Service**, quindi selezionare **Accedi**.
2. Selezionare **Amministratore** dal menu a discesa **Nome utente**.
3. Fare clic su **Password dimenticata?**
4. Immettere la risposta alla domanda di sicurezza visualizzata, quindi fare clic su **Genera password**. Viene visualizzato un messaggio contenente la password. Se si dimentica la risposta alla domanda di sicurezza, occorre disinstallare McAfee Privacy Service in Modalità provvisoria (solo Windows 2000 e Windows XP).

L'utente di avvio

Per l'utente di avvio l'accesso a Privacy Service viene effettuato automaticamente all'avvio del computer.

Se, ad esempio, un utente utilizza il computer o Internet più di altri, è possibile impostarlo come utente di avvio. Per l'utente di avvio che utilizza il computer non è necessario effettuare l'accesso a Privacy Service.

Chi ha bambini piccoli può impostare il più piccolo come utente di avvio. In questo modo, gli utenti più grandi che utilizzano il computer possono disconnettersi dall'account dell'utente più giovane ed effettuare l'accesso con il proprio nome utente e la propria password. Ciò permette di proteggere gli utenti più giovani dalla visione di siti Web inappropriati.

Apertura di McAfee Privacy Service

Quando si installa McAfee Privacy Service, l'icona McAfee viene visualizzata nella barra delle applicazioni di Windows, accanto all'orologio del sistema. Dall'icona McAfee è possibile accedere a McAfee Privacy Service, a McAfee SecurityCenter e ad altri prodotti McAfee installati nel computer.

Apertura e accesso a Privacy Service

Per aprire Privacy Service:

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **McAfee Privacy Service**, quindi selezionare **Accedi**.
2. Selezionare il nome utente dal menu a discesa **Nome utente**.
3. Immettere la password nel campo **Password**.
4. Fare clic su **Accedi**.

Disattivazione di Privacy Service

Per disattivare Privacy Service è necessario avere effettuato l'accesso come amministratore.

Per disattivare Privacy Service:

Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **McAfee Privacy Service**, quindi selezionare **Chiudi sessione**.

NOTA
Se al posto di **Chiudi sessione** viene visualizzato **Accedi**, la disconnessione è già stata effettuata.

Aggiornamento di McAfee Privacy Service

Mentre il computer è attivo e collegato a Internet, McAfee SecurityCenter controlla regolarmente la disponibilità di aggiornamenti di Privacy Service. Se è disponibile un aggiornamento, McAfee SecurityCenter richiede di aggiornare Privacy Service.

Per controllare manualmente se vi sono aggiornamenti disponibili, fare clic sull'icona Aggiornamenti nel riquadro superiore.

Aggiunta di utenti

Per aggiungere utenti è necessario effettuare l'accesso a Privacy Service come amministratore.

1. Fare clic con il pulsante destro del mouse sull'icona McAfee nella barra delle applicazioni di Windows.
2. Scegliere **McAfee Privacy Service**, quindi selezionare **Gestisci utenti**. Viene visualizzata la finestra di dialogo **Selezionare un utente**.
3. Fare clic su **Aggiungi** e immettere il nome del nuovo utente nel campo **Nome utente**.

Impostazione della password

1. Immettere una password nel campo **Password**. La password può essere costituita da un massimo di 50 caratteri e può contenere numeri e lettere minuscole e maiuscole.
2. Immettere nuovamente la password nel campo **Conferma password**.
3. Selezionare **Imposta utente come utente di avvio** se si desidera che l'utente sia l'utente di avvio.
4. Fare clic su **Avanti**.

Quando si assegnano le password, tenere in considerazione l'età dell'utente. Se, ad esempio, si assegna una password a un bambino, creare una password semplice. Se si assegna una password a un ragazzo o a un adulto, creare una password più complessa.

Impostazione del gruppo di età

Selezionare l'impostazione appropriata basata sull'età, quindi fare clic su **Avanti**.

Impostazione del blocco dei cookie

Selezionare l'opzione appropriata, quindi fare clic su **Avanti**.

- **Rifiuta tutti i cookie:** rende i cookie illeggibili per i siti Web che li hanno inviati. Alcuni siti Web richiedono l'attivazione dei cookie per poter funzionare correttamente.
- **Richiedi a utente se accettare i cookie:** consente di decidere di volta in volta se accettare o rifiutare i cookie. Privacy Service notifica all'utente quando un sito Web che sta per essere visualizzato tenta di inviare un cookie al computer. Una volta effettuata la scelta, non verrà chiesto nuovamente di accettare quel cookie.
- **Accetta tutti i cookie:** consente ai siti Web di leggere i cookie inviati al computer.

> **NOTA**
> Alcuni siti Web richiedono l'attivazione dei cookie per poter funzionare correttamente.
>
> Privacy Service accetta sempre i cookie provenienti da McAfee.

Impostazione delle limitazioni degli orari di accesso a Internet

Per concedere l'utilizzo illimitato di Internet:

1. Selezionare **Utilizzo illimitato di Internet**.
2. Fare clic su **Crea**. Il nuovo utente viene visualizzato nell'elenco Selezionare un utente.

Per concedere l'utilizzo limitato di Internet:

1. Selezionare **Utilizzo limitato di Internet**, quindi fare clic su **Modifica**.
2. Nella pagina Limitazioni degli orari di accesso a Internet, trascinare la griglia per selezionare i giorni e gli orari durante i quali un utente potrà accedere a Internet.
   È possibile specificare le limitazioni degli orari di accesso per intervalli di trenta minuti. Le parti verdi della griglia indicano i periodi di tempo in cui l'utente può accedere a Internet. Le parti rosse, al contrario, indicano i momenti in cui l'utente non può accedere a Internet. Se un utente tenta di utilizzare Internet in un orario non consentito, viene visualizzato un messaggio che informa che l'utilizzo di Internet in quel momento non è permesso. Per modificare i periodi durante i quali un utente può accedere a Internet, trascinare le parti verdi della griglia.
3. Fare clic su **Fine**.

4 Fare clic su **Crea**. Il nuovo utente viene visualizzato nella pagina Selezionare un utente. Se un utente tenta di utilizzare Internet in un orario non consentito, viene visualizzato un messaggio che informa che l'utilizzo di Internet in quel momento non è permesso.

Per proibire l'utilizzo di Internet:

- Selezionare **Utilizzo limitato di Internet**, quindi fare clic su **Crea**. Quando l'utente utilizza il computer, gli verrà chiesto di effettuare l'accesso a Privacy Service. Potrà utilizzare il computer, ma non Internet.

Modifica di utenti

Per modificare gli utenti è necessario effettuare l'accesso a Privacy Service come amministratore.

Modifica delle password

1 Selezionare l'utente di cui si desidera modificare le informazioni, quindi fare clic su **Modifica**.

2 Selezionare **Password**, quindi immettere la nuova password dell'utente nel campo **Nuova password**. La password può essere costituita da un massimo di 50 caratteri e può contenere numeri e lettere minuscole e maiuscole.

3 Immettere la medesima password nel campo **Conferma password**, quindi fare clic su **Applica**.

4 Fare clic su **OK** nella finestra di dialogo di conferma.

NOTA
Un amministratore può modificare la password di un utente senza conoscerla.

Modifica delle informazioni di un utente

1 Selezionare l'utente di cui si desidera modificare le informazioni, quindi fare clic su **Modifica**.

2 Selezionare **Informazioni utente**.

3 Immettere il nuovo nome utente nel campo **Nuovo nome utente**.

4 Fare clic su **Applica**, quindi su **OK** nella finestra di dialogo di conferma.

5 Per limitare la visualizzazione dei siti Web di un utente all'elenco dei siti Web consentiti, selezionare **Limitare l'accesso dell'utente ai siti Web presenti in "Siti Web autorizzati"**.

Modifica dell'impostazione di blocco dei cookie

1. Selezionare l'utente di cui si desidera modificare le informazioni, quindi fare clic su **Modifica**.
2. Selezionare **Cookie**, quindi l'opzione desiderata.
   - **Rifiuta tutti i cookie:** rende i cookie illeggibili per i siti Web che li hanno inviati. Alcuni siti Web richiedono l'attivazione dei cookie per poter funzionare correttamente.
   - **Richiedi a utente se accettare i cookie:** consente di decidere di volta in volta se accettare o rifiutare i cookie. Privacy Service notifica all'utente quando un sito Web che sta per essere visualizzato tenta di inviare un cookie al computer. Una volta effettuata la scelta, non verrà chiesto nuovamente di accettare quel cookie.
   - **Accetta tutti i cookie:** consente ai siti Web di leggere i cookie inviati al computer.
3. Fare clic su **Applica**, quindi su **OK** nella finestra di dialogo di conferma.

Modifica dell'elenco dei cookie accettati e rifiutati

1. Selezionare **Richiedi a utente se accettare i cookie**, quindi fare clic su **Modifica** per specificare quali siti Web sono autorizzati a leggere i cookie.
2. Specificare l'elenco che si sta modificando selezionando **Siti Web che possono impostare cookie** o **Siti Web che non possono impostare cookie**.
3. Immettere nel campo **http://** l'indirizzo del sito Web da cui si accettano o rifiutano i cookie.
4. Fare clic su **Aggiungi**. Il sito Web viene visualizzato nell'elenco relativo.
5. Fare clic su **Fine** al termine delle modifiche.

NOTA
Alcuni siti Web richiedono l'attivazione dei cookie per poter funzionare correttamente.

Privacy Service accetta sempre i cookie provenienti da McAfee.

Modifica del gruppo di età

1. Selezionare l'utente di cui si desidera modificare le informazioni, quindi fare clic su **Modifica**.
2. Selezionare **Gruppo di età**.
3. Selezionare un nuovo gruppo di età per l'utente, quindi fare clic su **Applica**.
4. Fare clic su **OK** nella finestra di dialogo di conferma.

Modifica delle limitazioni degli orari di accesso a Internet

1. Selezionare l'utente di cui si desidera modificare le informazioni, quindi fare clic su **Modifica**.
2. Selezionare **Limitazioni orari di accesso** ed effettuare le seguenti operazioni:

Per consentire all'utente l'accesso continuo a Internet:

1. Selezionare **Utilizzo illimitato di Internet**, quindi fare clic su **Applica**.
2. Fare clic su **OK** nella finestra di dialogo di conferma.

Per limitare l'accesso a Internet dell'utente:

1. Selezionare **Utilizzo limitato di Internet**, quindi fare clic su **Modifica**.
2. Nella pagina Limitazioni degli orari di accesso a Internet, selezionare un quadrato verde o rosso e trascinare la griglia per modificare i giorni e gli orari durante i quali un utente potrà accedere a Internet.
   È possibile specificare le limitazioni degli orari di accesso per intervalli di trenta minuti. Le parti verdi della griglia indicano i periodi di tempo in cui l'utente può accedere a Internet. Le parti rosse, al contrario, indicano i momenti in cui l'utente non può accedere a Internet. Se un utente tenta di utilizzare Internet in un orario non consentito, viene visualizzato un messaggio che informa che l'utilizzo di Internet in quel momento non è permesso.
3. Fare clic su **Applica**.
4. Nella pagina Limitazioni orari di accesso, fare clic su **OK**.
5. Fare clic su **OK** nella finestra di conferma di McAfee Privacy Service.

Modifica dell'utente di avvio

1. Selezionare l'utente che si desidera designare come utente di avvio, quindi fare clic su **Modifica**.
2. Selezionare **Informazioni utente**.
3. Selezionare **Imposta utente come utente di avvio**.
4. Fare clic su **Applica**, quindi su **OK** nella finestra di dialogo di conferma.

> **NOTA**
> Se esiste già un utente di avvio, non è necessario deselezionarlo.

Rimozione di utenti

1. Selezionare l'utente da rimuovere, quindi fare clic su **Rimuovi**.
2. Fare clic su **Sì** nella finestra di dialogo di conferma.
3. Al termine delle modifiche, chiudere la finestra di Privacy Service.

Opzioni

Per configurare le opzioni di Privacy Service è necessario accedervi come amministratore.

Blocco di siti Web

1. Fare clic su **Opzioni**, quindi selezionare **Elenco Blocca**.
2. Immettere nel campo **http://** l'URL del sito Web che si desidera bloccare, quindi fare clic su **Aggiungi**. Il sito Web viene visualizzato nell'elenco **Siti Web bloccati**.

> **NOTA**
> Gli utenti (inclusi gli amministratori) che appartengono al gruppo degli utenti adulti possono accedere a tutti i siti Web, compresi quelli presenti nell'elenco Siti Web bloccati. Per verificare i siti Web bloccati, gli amministratori devono effettuare l'accesso come utenti non adulti.

Autorizzazione di siti Web

L'amministratore può consentire a tutti gli utenti di visualizzare dei siti Web specifici. Le impostazioni predefinite di Privacy Service verranno ignorate e i siti Web verranno aggiunti all'elenco Blocca.

1. Fare clic su **Opzioni**, quindi selezionare **Elenco Autorizza**.
2. Immettere nel campo **http://** l'indirizzo del sito Web che si desidera autorizzare, quindi fare clic su **Aggiungi**. Il sito Web viene visualizzato nell'elenco **Siti Web autorizzati**.

Blocco di informazioni

L'amministratore può impedire ad altri utenti di inviare informazioni personali specifiche via Internet (l'amministratore può però inviarle).

Quando vengono rilevate informazioni di identificazione personale (PII) in un oggetto che sta per essere inviato, si verificherà quanto segue:

- Per l'amministratore, viene visualizzato un messaggio che consente di decidere se inviare o meno le informazioni.
- Se l'utente collegato non è l'amministratore, le informazioni bloccate vengono sostituite da *MFEMFEMFE*. Se, ad esempio, si invia il messaggio di posta elettronica *Lance Armstrong vince il giro* e Armstrong è impostato come informazione personale da bloccare, il messaggio di posta elettronica effettivamente inviato sarà *Lance MFEMFEMFE vince il giro*.

Aggiunta di informazioni

1. Fare clic su **Opzioni**, quindi selezionare **Blocca informazioni**.
2. Fare clic su **Aggiungi**. Viene visualizzato il menu a discesa **Seleziona tipo**.
3. Selezionare il tipo di informazioni che si desidera bloccare.
4. Immettere le informazioni negli appositi campi, quindi fare clic su **OK**. Le informazioni immesse vengono visualizzate nell'elenco.

Modifica di informazioni

1. Fare clic su **Opzioni**, quindi selezionare **Blocca informazioni**.
2. Selezionare le informazioni che si desidera modificare, quindi fare clic su **Modifica**.
3. Apportare le dovute modifiche, quindi fare clic su **OK**. Se non è necessario modificare le informazioni, fare clic su **Annulla**.

Rimozione di informazioni personali

1. Fare clic su **Opzioni**, quindi selezionare **Blocca informazioni**.
2. Selezionare le informazioni che si desidera rimuovere, quindi fare clic su **Rimuovi**.
3. Fare clic su **Sì** nella finestra di dialogo di conferma.

Blocco di Web bug

I Web bug sono piccoli file grafici in grado di inviare messaggi a terzi, di registrare le abitudini di navigazione in Internet e di trasmettere informazioni personali a un database esterno. Chi riceve queste informazioni le può utilizzare per creare dei profili utente.

Per impedire ai Web bug di essere caricati all'interno delle pagine Web visitate, selezionare **Blocca Web bug su questo computer**.

Blocco della pubblicità

I messaggi pubblicitari sono in genere immagini inviate da un dominio terzo a una pagina Web o una finestra popup. Privacy Service non blocca la pubblicità inviata dallo stesso dominio della pagina Web host.

I popup sono finestre secondarie del browser che presentano messaggi pubblicitari indesiderati, visualizzati automaticamente quando si visita un sito Web. Privacy Service blocca solo i popup caricati automaticamente quando viene caricata una pagina Web. I popup attivati dalla selezione di un collegamento non vengono bloccati da Privacy Service. Per visualizzare un popup bloccato, tenere premuto il tasto CTRL e aggiornare la pagina Web.

Configurare Privacy Service in modo da bloccare pubblicità e popup quando si utilizza Internet.

1. Fare clic su **Opzioni**, quindi selezionare **Blocca pubblicità**.
2. Selezionare l'opzione desiderata.
   - **Blocca pubblicità su questo computer:** blocca la pubblicità quando si utilizza Internet.
   - **Blocca popup su questo computer:** blocca i popup quando si utilizza Internet.
3. Fare clic su **Applica**, quindi su **OK** nella finestra di dialogo di conferma.

Per disattivare il blocco dei popup, fare clic con il pulsante destro del mouse sulla pagina Web, scegliere **Funzione di blocco dei popup di McAfee**, quindi deselezionare **Attiva funzione di blocco dei popup**.

Autorizzazione di cookie da siti Web specifici

Se si bloccano i cookie o si richiede di essere avvisati prima che vengano accettati, ma determinati siti Web non funzionano correttamente, è possibile configurare Privacy Service in modo da autorizzare il sito alla lettura dei cookie.

1. Fare clic su **Opzioni**, quindi selezionare **Cookie**.
2. Immettere nel campo **http://** l'indirizzo del sito Web che necessita la lettura dei cookie, quindi fare clic su **Aggiungi**. L'indirizzo viene visualizzato nell'elenco **Accetta siti Web con cookie**.

Registro eventi

Per visualizzare il registro degli eventi è necessario effettuare l'accesso a Privacy Service come amministratore. Selezionare **Registro eventi**, quindi fare clic su una voce del registro per visualizzarne i dettagli. Per salvare o visualizzare un registro salvato, selezionare la scheda Registri salvati.

Data e ora

Per impostazione predefinita, nel Registro eventi le informazioni vengono visualizzate in ordine cronologico, con gli eventi più recenti per primi. Se le voci del Registro eventi non sono in ordine cronologico, fare clic sull'intestazione Data e ora.

La data è visualizzata nel formato giorno/mese/anno e l'ora nel formato ora:minuti:secondi.

Utente

L'utente è la persona che aveva effettuato l'accesso e stava utilizzando Internet nel momento in cui l'evento è stato registrato da Privacy Service.

Riepilogo

I riepiloghi forniscono una descrizione rapida e concisa delle operazioni effettuate da Privacy Service per proteggere gli utenti e delle operazioni effettuate dagli utenti su Internet.

Dettagli evento

Nel campo Dettagli evento vengono visualizzati i dettagli delle voci.

Salvataggio del registro corrente

La pagina Registro corrente mostra informazioni relative alle operazioni effettuate di recente da amministratori e utenti. Tali informazioni possono essere salvate per essere visualizzate in un secondo momento.

Per salvare un registro eventi corrente

1. Effettuare l'accesso a Privacy Service come amministratore.
2. Selezionare **Registro eventi**.
3. Nella pagina Registro corrente, fare clic su **Salva registro**.
4. Digitare il nome del file di registro nel campo **Nome file**.
5. Fare clic su **Salva**.

Visualizzazione dei registri salvati

La pagina Registro corrente mostra informazioni relative alle operazioni effettuate di recente da amministratori e utenti. Tali informazioni possono essere salvate per essere visualizzate in un secondo momento.

Per visualizzare un registro salvato

1. Effettuare l'accesso a Privacy Service come amministratore.
2. Selezionare **Registro eventi**.
3. Nella pagina Registro corrente, fare clic su **Apri registro**.
4. Nella finestra di dialogo **Seleziona registro salvato da visualizzare**, selezionare il file database di backup e fare clic su **Apri**.

Utilità

Per accedere alle utilità è necessario effettuare l'accesso a Privacy Service come amministratore, quindi fare clic su **Utilità**.

Per rimuovere file, cartelle o l'intero contenuto di un disco, fare clic su **McAfee Shredder**. Per salvare le impostazioni del database di Privacy Service, fare clic su **Backup**. Per ripristinare le impostazioni, fare clic su **Ripristina**.

Cancellazione definitiva di file con McAfee Shredder

McAfee Shredder protegge la privacy grazie alla cancellazione rapida e sicura dei file indesiderati.

I file eliminati possono essere recuperati dal computer anche dopo che il Cestino è stato svuotato. Quando si elimina un file, lo spazio da esso occupato sull'unità disco viene semplicemente contrassegnato come non più in uso, ma il file fisicamente esiste ancora.

Perché in Windows rimangono residui di file

Per eliminare definitivamente un file, occorre sovrascriverlo ripetutamente con nuovi dati. Se in Microsoft Windows i file venissero eliminati in modo sicuro, ciascuna operazione sui file risulterebbe molto lenta. La distruzione di un documento non ne impedisce sempre il recupero perché alcuni programmi creano copie temporanee nascoste dei documenti aperti. Se si distruggono solo i documenti visibili in Esplora risorse, è possibile che ne esistano ancora delle copie temporanee. Si consiglia di eseguire Shredder periodicamente sullo spazio libero dell'unità disco per assicurarsi che tali copie temporanee siano eliminate definitivamente.

NOTA
Appositi strumenti informatici del sistema giudiziario consentono di recuperare dichiarazioni dei redditi, riepiloghi di lavori o altri documenti eliminati.

Elementi che è possibile cancellare con McAfee Shredder

McAfee Shredder consente di cancellare in modo sicuro e definitivo:

- Uno o più file o cartelle
- Un intero disco
- Le tracce dell'esplorazione del Web

Cancellazione definitiva dei file in Esplora risorse

Per distruggere un file da Esplora risorse:

1. Aprire Esplora risorse, quindi selezionare il file o i file da distruggere.
2. Fare clic con il pulsante destro del mouse sugli elementi selezionati, scegliere **Invia a**, quindi selezionare **McAfee Shredder**.

Come svuotare il Cestino di Windows

Se i file sono nel Cestino, McAfee Shredder offre un metodo più sicuro per svuotarlo.

Per distruggere il contenuto del Cestino:

1. Nel desktop di Windows, fare clic con il pulsante destro del mouse sul Cestino.
2. Selezionare **Distruggi contenuto del Cestino**, quindi seguire le istruzioni visualizzate.

Personalizzazione delle impostazioni di Shredder

È possibile:

- Specificare il numero di passaggi di distruzione.
- Mostrare un messaggio di avviso quando si distruggono i file.
- Individuare eventuali errori nel disco rigido prima della distruzione.
- Aggiungere McAfee Shredder al menu Invia a.
- Aggiungere un'icona di Shredder al desktop di Windows.

Per personalizzare le impostazioni di Shredder, aprire McAfee Shredder, fare clic su **Proprietà**, quindi seguire le istruzioni visualizzate.

Backup del database di Privacy Service

È possibile ripristinare il database di Privacy Service in due modi: se il database di Privacy Service viene danneggiato o eliminato, ne viene richiesto il ripristino, altrimenti è possibile ripristinare le impostazioni del database durante l'esecuzione di Privacy Service.

1. Fare clic su **Utilità**, quindi selezionare **Backup**.
2. Fare clic su **Sfoglia** per selezionare il percorso per il file database, quindi fare clic su **OK**.
3. Immettere una password nel campo **Password**.
4. Immettere nuovamente la password nel campo **Conferma password**, quindi fare clic su **Backup**.
5. Fare clic su **OK** nella finestra di dialogo di conferma.
6. Al termine, chiudere la finestra di Privacy Service.

> **NOTA**
> Mantenere segreta la password e non dimenticarla. Senza la password non è possibile ripristinare le impostazioni di Privacy Service.

Ripristino del database di backup

1 Il ripristino delle impostazioni originali di Privacy Service può essere effettuato in due modi:

- Caricando il database di backup in seguito alla richiesta di ripristinare le impostazioni a causa del danneggiamento o dell'eliminazione del database.
- Caricando il database di backup durante l'esecuzione di Privacy Service.

Per ripristinare le impostazioni di Privacy Service in seguito ad un messaggio di richiesta:

1 Fare clic su **Sfoglia** per individuare il file.

2 Digitare la password nel campo **Password**.

3 Fare clic su **Ripristina**.
Se non si è creata una copia di backup del database di Privacy Service, se si è dimenticata la password di backup o se il ripristino del database non funziona, disinstallare e reinstallare Privacy Service.

Per ripristinare le impostazioni di Privacy Service durante la sua esecuzione:

1 Fare clic sulla scheda **Utilità**.

2 Fare clic su **Ripristina**.

3 Fare clic su **Sfoglia** e digitare il percorso e il nome del file di backup.

4 Fare clic su **Apri**.

5 Digitare la password nel campo **Password**.

6 Fare clic su **Ripristina**, quindi su **OK** nella finestra di conferma di McAfee Privacy Service.

Opzioni utente

Queste istruzioni non sono rivolte all'amministratore.

È possibile cambiare sia la password che il nome utente. Si consiglia di cambiare la password fornita dall'amministratore e di modificarla una volta al mese, o qualora si ritenga che sia nota ad altri utenti. In tal modo si impedirà ad estranei di utilizzare Internet con il proprio nome utente.

Modifica della password

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **Privacy Service**, quindi selezionare **Opzioni**.
2. Fare clic su **Password**, quindi immettere la vecchia password nel campo **Vecchia password**.
3. Immettere la nuova password nel campo **Nuova password**.
4. Reimmettere la nuova password nel campo **Conferma password**, quindi fare clic su **Applica**.
5. Fare clic su **OK** nella finestra di dialogo di conferma. Si dispone ora di una nuova password.

Modifica del nome utente

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **Privacy Service**, quindi selezionare **Opzioni**.
2. Fare clic su **Informazioni utente**.
3. Immettere il nuovo nome utente nel campo **Nuovo nome utente**, quindi fare clic su **Applica**.
4. Fare clic su **OK** nella finestra di dialogo di conferma. Si dispone ora di un nuovo nome utente.

Cancellazione della cache

Si consiglia di cancellare la cache, per assicurarsi che un bambino non acceda alle pagine Web visitate recentemente. Per cancellare la cache, effettuare le seguenti operazioni:

1. Aprire Internet Explorer.
2. Scegliere **Opzioni Internet** nel menu **Strumenti**. Verrà aperta la finestra di dialogo Opzioni Internet.
3. Nella sezione **File temporanei Internet**, fare clic su **Elimina file**. Verrà visualizzata la finestra di dialogo Eliminazione file.
4. Selezionare la casella di controllo **Elimina tutto il contenuto non in linea**, quindi fare clic su **OK**.
5. Fare clic su **OK** per chiudere la finestra di dialogo Opzioni Internet.

Accettazione di cookie

Questa opzione è disponibile solo se l'amministratore consente di accettare o rifiutare i cookie quando vengono intercettati.

Se si accede a siti Web che richiedono i cookie, è possibile consentire a tali siti l'autorizzazione a leggere i cookie.

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **Privacy Service**, quindi selezionare **Opzioni**.
2. Fare clic su **Cookie accettati**.
3. Immettere nel campo **http://** l'URL del sito Web, quindi fare clic su **Aggiungi**. Il sito Web viene visualizzato nell'elenco **Sito Web**.

Per rimuovere un sito Web dall'elenco:

1. Selezionare l'URL del sito Web dall'elenco **Sito Web**.
2. Fare clic su **Rimuovi**, quindi fare clic su **Sì** nella finestra di dialogo di conferma.

Rifiuto di cookie

Questa opzione è disponibile solo se l'amministratore consente di accettare o rifiutare i cookie quando vengono intercettati.

Se si accede a siti Web che non richiedono i cookie, è possibile rifiutarli senza che ciò venga richiesto.

1. Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **Privacy Service**, quindi selezionare **Opzioni**.
2. Fare clic su **Cookie rifiutati**.
3. Immettere nel campo **http://** l'URL del sito Web, quindi fare clic su **Aggiungi**. Il sito Web viene visualizzato nell'elenco **Sito Web**.

Per rimuovere un sito Web dall'elenco:

1. Selezionare l'URL del sito Web dall'elenco **Sito Web**.
2. Fare clic su **Rimuovi**, quindi fare clic su **Sì** nella finestra di dialogo di conferma.

McAfee SpamKiller 5

Benvenuti in McAfee SpamKiller.

McAfee SpamKiller consente di evitare che la posta indesiderata arrivi nella propria cartella di posta in arrivo. Grazie a questo software, è possibile usufruire delle seguenti funzioni:

Funzioni

Nella presente versione di SpamKiller sono disponibili le funzioni seguenti:

- Filtraggio: le opzioni di filtraggio avanzate forniscono nuove tecniche di filtraggio, inclusi il supporto per il filtraggio di metacaratteri e l'identificazione dei testi indesiderati.
- Phishing: tramite una barra degli strumenti di Internet Explorer, il browser plug-in AntiPhishing identifica e blocca facilmente potenziali siti Web che operano il phishing.
- Integrazione di Microsoft Outlook e Outlook Express: tramite la barra degli strumenti è disponibile una cartella all'interno del client di posta elettronica che consente di bloccare i messaggi indesiderati.
- Installazione: installazione e configurazione facilitate. Il rilevamento automatico dell'account garantisce una installazione, una configurazione e una integrazione con gli account di posta elettronica esistenti prive di problemi.
- Aggiornamenti: gli aggiornamenti automatici vengono eseguiti in modo invisibile in background, sempre garantendo la protezione per ridurre al minimo l'esposizione del sistema a minacce di spamming emergenti.
- Interfaccia: interfaccia utente intuitiva che facilita la gestione di un sistema privo di messaggi indesiderati.
- Supporto: supporto tecnico gratuito tramite messaggistica immediata e posta elettronica per semplificare e velocizzare l'assistenza clienti prestata così dal vivo.

Elaborazione dei messaggi indesiderati: per impostazione predefinita i messaggi indesiderati vengono contrassegnati con il tag [SPAM] e spostati nella cartella SpamKiller di Outlook e Outlook Express oppure in Posta in arrivo. I messaggi contrassegnati vengono visualizzati anche nella pagina Posta accettata.

Opzioni utente

- Blocco dei messaggi indesiderati mediante filtri e messa in quarantena della posta indesiderata al di fuori della cartella Posta in arrivo
- Visualizzazione dei messaggi bloccati e di quelli accettati
- Monitoraggio e applicazione di filtri a più account di posta elettronica
- Importazione di indirizzi nell'elenco degli amici
- Introduzione di provvedimenti per ostacolare i mittenti di messaggi indesiderati (segnalazione dei messaggi indesiderati, reclami relativi alla posta indesiderata, creazione di filtri personalizzati)
- Protezione dei minori dalla visualizzazione di messaggi indesiderati
- Blocco e recupero con un solo clic del mouse
- Supporto del set di caratteri a byte doppio
- Supporto multiutente (per Windows 2000 e Windows XP)

Filtri

- Aggiornamento automatico dei filtri
- Creazione di filtri personalizzati per bloccare i messaggi di posta elettronica contenenti principalmente immagini, testo invisibile o formattazione non valida
- Filtraggio principale a più livelli
- Filtro su attacchi di tipo dictionary
- Filtraggio adattivo multilivello
- Filtri di protezione

Informazioni sul riquadro superiore

Nel riquadro superiore di tutte le pagine di SpamKiller sono presenti le icone seguenti:

- Fare clic su **Cambia utente** per accedere con un altro nome utente.

  Nota: l'icona **Cambia utente** è disponibile solo se il sistema del computer in uso è Windows 2000 o Windows XP, se sono stati aggiunti più utenti a SpamKiller e se si è connessi al programma in qualità di amministratore.

- Fare clic su **Supporto** per aprire la pagina relativa al supporto online di McAfee, che fornisce informazioni importanti su SpamKiller e altri prodotti McAfee, risposte alle domande frequenti e altro ancora. Per accedere alla pagina relativa al supporto è necessario essere connessi a Internet.
- Fare clic su **Guida in linea** per aprire la Guida in linea, nella quale sono contenute istruzioni dettagliate sulla configurazione e l'utilizzo di SpamKiller.

Dopo aver installato SpamKiller, l'icona McAfee viene inclusa nella barra delle applicazioni di Windows, accanto all'orologio del sistema. Dall'icona McAfee è possibile accedere a SpamKiller, McAfee SecurityCenter e altri prodotti McAfee installati nel sistema.

Disattivazione di SpamKiller

È possibile disattivare SpamKiller ed evitare che i messaggi di posta elettronica vengano filtrati.

Per disattivare i filtri:

Fare clic con il pulsante destro del mouse sull'icona McAfee , scegliere **SpamKiller** e fare clic su **Disattiva**. Oppure fare clic sulla scheda **Riepilogo**, quindi su **Fare clic qui per disattivare**.

Per attivare i filtri:

Fare clic con il pulsante destro del mouse sull'icona McAfee, scegliere **SpamKiller** e fare clic su **Attiva**. Oppure fare clic sulla scheda **Riepilogo**, quindi su **Fare clic qui per attivare**.

Informazioni sulla pagina Riepilogo

Fare clic sulla scheda **Riepilogo** per aprire la pagina Riepilogo (Figura 5-11).

- La sezione **Panoramica dello stato di SpamKiller** indica se il filtraggio è attivato, la data dell'ultimo aggiornamento di un elenco degli amici e il numero di messaggi indesiderati ricevuti nella giornata. In questa pagina è possibile attivare o disattivare il filtraggio di SpamKiller, aggiornare gli elenchi degli amici e aprire la pagina Posta bloccata.
- La sezione **Messaggi di posta elettronica più recenti identificati come indesiderati e bloccati** include gli ultimi messaggi indesiderati bloccati da SpamKiller (e rimossi da Posta in arrivo).
- La sezione **Panoramica posta** visualizza il numero totale di messaggi di posta elettronica, i messaggi indesiderati (bloccati) e la percentuale di messaggi indesiderati totali ricevuti.

- La sezione **Messaggi indesid. recenti** fornisce un dettaglio del tipo di messaggi indesiderati ricevuti negli ultimi 30 giorni.

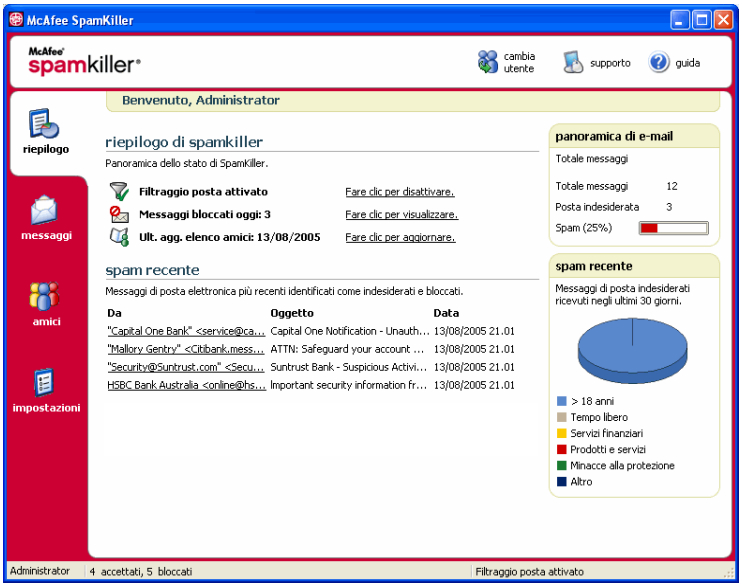


Figura 5-11. Pagina Riepilogo

Integrazione con Microsoft Outlook e Outlook Express

È possibile accedere alle funzioni principali di SpamKiller da Outlook Express 6.0, Outlook 98, Outlook 2000 e Outlook XP, selezionando il menu o la barra degli strumenti di SpamKiller.

A destra delle barre degli strumenti standard di Outlook e Outlook Express viene visualizzata la barra degli strumenti di SpamKiller. Se la barra degli strumenti non è visibile, espandere la finestra dell'applicazione di posta elettronica o fare clic sulle frecce per visualizzare ulteriori barre degli strumenti.

La prima volta che la barra degli strumenti di SpamKiller viene visualizzata nell'applicazione di posta elettronica, è possibile utilizzarne i comandi solo con i nuovi messaggi. I messaggi indesiderati esistenti devono essere eliminati manualmente.

Gestione degli utenti e degli account di posta elettronica

Questa sezione descrive come gestire gli account e gli utenti.

Aggiunta di account di posta elettronica

È possibile aggiungere i seguenti account di posta elettronica:

- Account di posta elettronica standard (POP3): la maggior parte degli utenti privati dispone di questo tipo di account.
- Account MSN/Hotmail: account MSN/Hotmail basati sul Web.

> **NOTA**
> Se il sistema in uso è Windows 2000 o Windows XP e si intende aggiungere più utenti in SpamKiller, occorre aggiungere gli utenti prima di poter aggiungere account di posta elettronica ai relativi profili utente. Per ulteriori informazioni, vedere *Aggiunta di utenti* a pagina 110. Se si aggiungono più utenti in SpamKiller, l'account viene aggiunto al profilo dell'utente attualmente collegato a SpamKiller.

Per aggiungere un account di posta elettronica:

1. Fare clic sulla scheda **Impostazioni** per aprire la pagina Impostazioni (Figura 5-12), quindi fare clic su **Account di posta elettronica**. Viene visualizzata la finestra di dialogo **Account di posta elettronica** in cui sono elencati tutti gli account aggiunti a SpamKiller.

   > **NOTA**
   > Se sono stati aggiunti più utenti in SpamKiller, l'elenco comprende gli account di posta elettronica dell'utente attualmente collegato a SpamKiller.

2. Fare clic su **Aggiungi**. Viene visualizzata la procedura guidata per gli account di posta elettronica.

   Attenersi alle istruzioni riportate nelle finestre di dialogo visualizzate.

Se si aggiunge un account MSN/Hotmail, SpamKiller cerca una rubrica di MSN/Hotmail da importare nell'elenco degli amici.

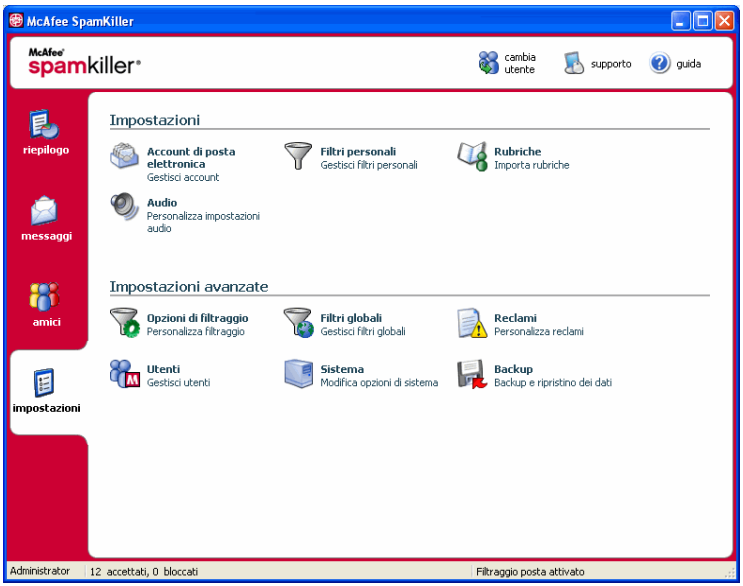


Figura 5-12. Pagina Impostazioni

Come indicare al programma il client di posta elettronica

Se si è aggiunto un account che SpamKiller non rileva (l'account non appare nella finestra di dialogo **Seleziona account**) o se si desidera leggere i messaggi MSN/Hotmail come un account POP3 in SpamKiller, indicare il client di posta elettronica a SpamKiller modificando il server della posta in arrivo.

Ad esempio, se il proprio server della posta in arrivo è “mail.mcafee.com”, modificarlo in “localhost”.

Eliminazione di account di posta elettronica

Eliminare un account di posta elettronica da SpamKiller se non si desidera più che venga filtrato da SpamKiller.

Eliminazione di un account di posta elettronica da SpamKiller

1 Fare clic sulla scheda **Impostazioni**, quindi selezionare **Account di posta elettronica**. Viene visualizzata la finestra di dialogo **Account di posta elettronica** in cui sono elencati tutti gli account aggiunti a SpamKiller.

> **NOTA**
> Se sono stati aggiunti più utenti in SpamKiller, l'elenco comprende gli account di posta elettronica dell'utente attualmente collegato a SpamKiller.

2 Selezionare un account e poi fare clic su **Elimina**.

Modifica delle proprietà degli account di posta elettronica

È possibile modificare le informazioni sugli account di posta elettronica aggiunti a SpamKiller. Ad esempio, è possibile modificare l'indirizzo di posta elettronica, la descrizione dell'account, le informazioni sul server, la frequenza con cui SpamKiller verifica se l'account ha ricevuto messaggi indesiderati e il modo in cui il sistema si collega a Internet.

Account POP3

Modifica di account POP3

1 Fare clic sulla scheda **Impostazioni**, quindi su **Account di posta elettronica**. Viene visualizzata la finestra di dialogo **Account di posta elettronica** in cui sono elencati tutti gli account aggiunti a SpamKiller.

> **NOTA**
> Se sono stati aggiunti più utenti in SpamKiller, l'elenco comprende gli account di posta elettronica dell'utente attualmente collegato a SpamKiller.

2 Selezionare un account POP3 e fare clic su **Modifica**.

3 Fare clic sulla scheda **Generale** per modificare la descrizione dell'account e l'indirizzo di posta elettronica.

- **Descrizione:** descrizione dell'account. In questa casella si può digitare qualunque informazione.
- **Indirizzo di posta elettronica:** indirizzo di posta elettronica dell'account.

4 Fare clic sulla scheda **Server** per modificare le informazioni sul server.

- **Posta in ingresso:** nome del server che riceve la posta in arrivo.
- **Nome utente:** nome utente usato per accedere all'account. Noto anche come Nome account.
- **Password:** password usata per accedere all'account.
- **Posta in uscita:** nome del server che invia la posta in uscita. Fare clic su **Altro** per modificare i requisiti di autenticazione del server di posta in uscita.

5 Fare clic sulla scheda **Verifica** per modificare la frequenza con cui SpamKiller verifica se l'account ha ricevuto messaggi indesiderati:

a Selezionare **Verifica ogni** oppure**Verifica ogni giorno alle**, quindi immettere o selezionare un orario nella casella corrispondente. Se si immette il numero zero, l'account verrà verificato da SpamKiller soltanto al momento della connessione.

b Selezionare ulteriori momenti in cui SpamKiller deve filtrare l'account:

Verifica all'avvio: se si dispone di una connessione diretta e si desidera che SpamKiller controlli l'account a ogni avvio del sistema.

Verifica quando si stabilisce una connessione: se si dispone di una connessione ad accesso remoto e si desidera che SpamKiller controlli l'account ogni volta che si stabilisce il collegamento a Internet.

6 Fare clic sulla scheda **Connessione** per specificare il modo in cui SpamKiller stabilisce una connessione a Internet così da controllare se nella cartella Posta in arrivo sono presenti nuovi messaggi da filtrare.

- **Non stabilire mai la connessione:** SpamKiller non stabilisce alcuna connessione automaticamente. Occorre prima stabilire manualmente la connessione ad accesso remoto.
- **Stabilisci la connessione quando necessario:** non è disponibile alcuna connessione a Internet, quindi SpamKiller tenta di collegarsi automaticamente tramite la connessione ad accesso remoto predefinita.
- **Stabilisci sempre la connessione:** SpamKiller tenta di collegarsi automaticamente mediante la connessione ad accesso remoto specificata.
- **Rimani connesso dopo il filtraggio:** il sistema resta collegato a Internet una volta che il filtraggio è stato completato.

7 Fare clic sulla scheda **Avanzate** per modificare le opzioni avanzate.

- **Lascia messaggi di posta indesiderati sul server:** se si desidera che una copia dei messaggi bloccati resti sul server di posta elettronica. È possibile visualizzare la posta dal client di posta elettronica e dalla pagina Posta bloccata di SpamKiller. Se la casella di controllo non è selezionata, i messaggi bloccati potranno essere visualizzati solo dalla pagina Posta bloccata.
- **Porta POP3:** (numero della porta POP3) il server POP3 gestisce i messaggi in arrivo.
- **Porta SMTP:** (numero della porta SMTP) il server SMTP gestisce i messaggi in uscita.
- **Timeout server:** tempo di attesa di SpamKiller per la ricezione di messaggi di posta elettronica prima del timeout e dell'interruzione.

  In caso di problemi nella ricezione della posta, aumentare il valore di timeout del server. La connessione di posta elettronica potrebbe essere lenta, quindi l'aumento del valore di timeout del server consente a SpamKiller di prolungare l'attesa prima del timeout.

8 Fare clic su **OK**.

Account MSN/Hotmail

Modifica di account MSN/Hotmail

1 Fare clic sulla scheda **Impostazioni**, quindi su **Account di posta elettronica**.

Viene visualizzata la finestra di dialogo **Account di posta elettronica** contenente l'elenco completo degli account di posta elettronica aggiunti a SpamKiller.

> **NOTA**
> Se sono stati aggiunti più utenti in SpamKiller, l'elenco comprende gli account di posta elettronica dell'utente attualmente collegato a SpamKiller.

2 Selezionare un account MSN/Hotmail e fare clic su **Modifica**.

3 Fare clic sulla scheda **Generale** per modificare la descrizione dell'account e l'indirizzo di posta elettronica.

- **Descrizione:** descrizione dell'account. In questa casella si può digitare qualunque informazione.
- **Indirizzo di posta elettronica:** indirizzo di posta elettronica dell'account.

4 Fare clic sulla scheda **Server** per modificare le informazioni sul server.

- **Posta in ingresso:** nome del server che riceve la posta in arrivo.
- **Password:** password usata per accedere all'account.
- **Posta in uscita:** nome del server che invia la posta in uscita.
- **Usa server SMTP per la posta in uscita:** selezionare questa opzione se si intende inviare messaggi di errore, senza includere la riga di firma MSN. La riga di firma MSN permette ai mittenti di messaggi indesiderati di capire più facilmente che si tratta di un messaggio d'errore fittizio.

  Fare clic su **Altro** per modificare i requisiti di autenticazione del server di posta in uscita.

5 Fare clic sulla scheda **Verifica** per specificare la frequenza con cui SpamKiller controlla se l'account ha ricevuto messaggi indesiderati:

a Selezionare **Verifica ogni** oppure **Verifica ogni giorno alle**, quindi immettere o selezionare un orario nella casella corrispondente. Se si immette il numero zero, l'account verrà verificato da SpamKiller soltanto al momento della connessione.

b Selezionare ulteriori momenti in cui SpamKiller deve filtrare l'account:

Verifica all'avvio: selezionare questa opzione se si dispone di una connessione diretta e si desidera che SpamKiller controlli l'account a ogni avvio del sistema.

Verifica quando si stabilisce una connessione: selezionare questa opzione se si dispone di una connessione ad accesso remoto e si desidera che SpamKiller controlli l'account ogni volta che si stabilisce il collegamento a Internet.

6 Fare clic sulla scheda **Connessione** per specificare il modo in cui SpamKiller stabilisce una connessione a Internet così da controllare se nella cartella Posta in arrivo sono presenti nuovi messaggi da filtrare.

- **Non stabilire mai la connessione:** SpamKiller non stabilisce alcuna connessione automaticamente. Occorre prima stabilire manualmente la connessione ad accesso remoto.
- **Stabilisci la connessione quando necessario:** quando non è disponibile alcuna connessione a Internet, SpamKiller tenta di collegarsi automaticamente tramite la connessione ad accesso remoto predefinita.
- **Stabilisci sempre la connessione:** SpamKiller tenta di collegarsi automaticamente mediante la connessione ad accesso remoto specificata.
- **Rimani connesso dopo il filtraggio:** il sistema resta collegato a Internet una volta che il filtraggio è stato completato.

7 Fare clic su **OK**.

Configurazione di un account Hotmail per il blocco dei messaggi indesiderati in Outlook o Outlook Express

SpamKiller è in grado di filtrare direttamente gli account Hotmail. Per ulteriori dettagli consultare la Guida in linea. Non è tuttavia possibile bloccare messaggi o aggiungere amici mediante la barra degli strumenti di SpamKiller in Outlook o Outlook Express fino a quando non si configura l'account Hotmail.

1. Configurare l'account Hotmail in MSK.
2. Se si dispone di un account Hotmail esistente in Outlook o Outlook Express, è necessario rimuoverlo.
3. Aggiungere l'account Hotmail a Outlook o Outlook Express. Verificare di selezionare **POP3** per il tipo di account e di server di posta elettronica in ingresso.
4. Assegnare al server in ingresso il nome **`localhost`**.
5. Digitare il nome del server SMTP in uscita disponibile (obbligatorio).
6. Completare il processo di configurazione dell'account. A questo punto è possibile bloccare i nuovi messaggi di posta indesiderati di Hotmail o aggiungere un amico.

Account MAPI

Per garantire l'integrazione di SpamKiller con MAPI in Outlook, è necessario che siano soddisfatte le seguenti condizioni:

- Solo per Outlook 98, Outlook deve essere stato installato con il supporto per società o gruppo di lavoro.
- Solo per Outlook 98, il primo account di posta elettronica deve essere un account MAPI.
- Il sistema deve essere connesso al dominio.

Modifica di account MAPI

1. Fare clic sulla scheda **Impostazioni**, quindi su **Account di posta elettronica**. Viene visualizzata la finestra di dialogo **Account di posta elettronica** in cui sono elencati tutti gli account aggiunti a SpamKiller.

   NOTA
   Se sono stati aggiunti più utenti in SpamKiller, l'elenco comprende gli account di posta elettronica dell'utente attualmente collegato a SpamKiller.

2. Selezionare un account MAPI e fare clic su **Modifica**.

3 Fare clic sulla scheda **Generale** per modificare la descrizione dell'account e l'indirizzo di posta elettronica.

- **Descrizione:** descrizione dell'account. In questa casella si può digitare qualunque informazione.
- **Indirizzo di posta elettronica:** indirizzo di posta elettronica dell'account.

4 Fare clic sulla scheda **Profilo** per modificare le informazioni del profilo.

- **Profilo:** profilo MAPI per l'account.
- **Password:** password corrispondente al profilo MAPI, se impostata (non necessariamente la password dell'account di posta elettronica).

5 Fare clic sulla scheda **Connessione** per specificare il modo in cui SpamKiller stabilisce una connessione a Internet così da controllare se nella cartella Posta in arrivo sono presenti nuovi messaggi da filtrare.

- **Non stabilire mai la connessione:** SpamKiller non stabilisce alcuna connessione automaticamente. Occorre prima stabilire manualmente la connessione ad accesso remoto.
- **Stabilisci la connessione quando necessario:** quando non è disponibile alcuna connessione a Internet, SpamKiller tenta di collegarsi automaticamente tramite la connessione ad accesso remoto predefinita.
- **Stabilisci sempre la connessione:** SpamKiller tenta di collegarsi automaticamente mediante la connessione ad accesso remoto specificata.
- **Rimani connesso dopo il filtraggio:** il sistema resta collegato a Internet una volta che il filtraggio è stato completato.

6 Fare clic su **OK**.

Aggiunta di utenti

SpamKiller è in grado di impostare più utenti, corrispondenti a quelli già impostati sul sistema operativo Windows 2000 o Windows XP.

Al momento dell'installazione di SpamKiller, è stato creato automaticamente un profilo amministratore per l'utente Windows che era collegato. Se durante l'installazione di SpamKiller sono stati aggiunti account di posta elettronica, questi sono stati aggiunti al profilo utente dell'amministratore.

Prima di aggiungere ulteriori account di posta elettronica in SpamKiller, è opportuno stabilire se aggiungere altri utenti di SpamKiller. L'aggiunta di utenti è utile se il sistema viene utilizzato da più persone, ciascuna con i propri account di posta elettronica. Gli account di posta elettronica di ciascun utente vengono aggiunti al rispettivo profilo, affinché ogni utente possa gestire i propri account di posta elettronica, le impostazioni personali, i filtri e l'elenco degli amici personali.

Le operazioni consentite in SpamKiller vengono definite in base al tipo di utente. Nella tabella riportata di seguito vengono riepilogate le autorizzazioni per ciascun tipo di utente. Gli amministratori possono eseguire tutte le operazioni, mentre gli utenti con limitazioni possono eseguire solo operazioni in base al proprio profilo personale. Ad esempio, gli amministratori possono visualizzare il contenuto completo dei messaggi bloccati, mentre gli utenti con limitazioni possono visualizzare solo la riga dell'oggetto.

Attività	Amministratore	Utente con limitazioni
Gestione degli account di posta elettronica, dei filtri, dell'elenco degli amici e delle impostazioni audio personali	X	X
Gestione delle pagine dei messaggi bloccati e dei messaggi accettati	X	X
Visualizzazione del testo dei messaggi bloccati	X	
Visualizzazione del testo dei messaggi accettati	X	X
Gestione dei filtri globali e dell'elenco degli amici globale	X	
Segnalazione di messaggi di posta indesiderati a McAfee	X	X
Invio di reclami e messaggi di errore	X	X
Gestione dei reclami e dei messaggi di errore (creazione, modifica ed eliminazione di modelli di messaggio)	X	
Gestione degli utenti (creazione, modifica ed eliminazione di utenti)	X	
Backup e ripristino di SpamKiller	X	
Visualizzazione della pagina di riepilogo dei messaggi indesiderati ricevuti	X	X

Quando un utente accede al sistema dopo essere stato aggiunto, viene invitato ad aggiungere un account di posta elettronica al proprio profilo utente.

Per aggiungere e gestire gli utenti, è necessario soddisfare i seguenti requisiti:

- Occorre essere collegati a SpamKiller in qualità di amministratore.
- Il sistema operativo deve essere Windows 2000 o Windows XP.
- Gli utenti che vengono aggiunti o gestiti devono disporre di account utente Windows.

Password utente e protezione dei minori dai messaggi indesiderati

La creazione di password utente aumenta il livello di riservatezza. Senza la password di connessione, un utente non può accedere alle impostazioni personali, l'elenco degli amici e l'elenco dei messaggi accettati di un altro utente. La creazione di password è utile, inoltre, per evitare che i minori accedano a SpamKiller e visualizzino il contenuto di messaggi indesiderati.

Creazione di una password per un utente di SpamKiller esistente

1. Fare clic sulla scheda **Impostazioni**, quindi su **Utenti**.
2. Selezionare un utente, quindi fare clic su **Modifica**.
3. Immettere una password nella casella **Password**. Quando l'utente accede a SpamKiller, deve usare la propria password.

   IMPORTANTE
   Se si dimentica la password, non è possibile recuperarla. Solo un amministratore di SpamKiller può creare una nuova password.

Aggiunta di un utente a SpamKiller

1. Fare clic sulla scheda **Impostazioni**, quindi su **Utenti**.
2. Fare clic su **Aggiungi**.

   Viene visualizzato un elenco di utenti Windows. Per aggiungere un utente che non è compreso nell'elenco, creare un account utente Windows per tale utente. Occorre, inoltre, che il nuovo utente si colleghi al sistema almeno una volta. In seguito, aggiungere l'utente in SpamKiller.

   NOTA
   Gli utenti Windows con privilegi di amministratore hanno privilegi di amministratore in SpamKiller.
3. Selezionare l'utente da aggiungere e fare clic su **OK**. L'utente viene aggiunto e il nome utente viene visualizzato nell'elenco degli utenti di SpamKiller.
4. Fare clic su **Chiudi** al termine dell'aggiunta degli utenti.

Per creare una password per un utente, vedere la sezione *Creazione di una password per un utente di SpamKiller esistente* a pagina 112.

Al successivo accesso dell'utente al sistema, viene richiesto di aggiungere un account di posta elettronica al profilo utente di SpamKiller. È possibile aggiungere account di posta elettronica al profilo utente se corrisponde a quello dell'utente collegato a SpamKiller e se si dispone delle informazioni necessarie sull'account. Per ulteriori informazioni, vedere la sezione *Aggiunta di account di posta elettronica* a pagina 103.

Modifica di un profilo utente di SpamKiller

1. Fare clic sulla scheda **Impostazioni**, quindi scegliere **Utenti**. Viene visualizzato un elenco di utenti di SpamKiller.
2. Selezionare un utente, quindi fare clic su **Modifica**.
3. Digitare un nuovo nome e una password.

Eliminazione di un profilo utente di SpamKiller

> **ATTENZIONE**
> Quando si elimina un profilo utente, si eliminano da SpamKiller anche gli account di posta elettronica di quell'utente.

1. Fare clic sulla scheda **Impostazioni**, quindi scegliere **Utenti**. Viene visualizzato un elenco di utenti di SpamKiller.
2. Selezionare un utente nell'elenco e fare clic su **Elimina**.

Accesso a SpamKiller in un ambiente multiutente

Quando gli utenti accedono al sistema e avviano SpamKiller, si collegano automaticamente a SpamKiller con il proprio profilo utente. Se agli utenti sono state assegnate delle password di SpamKiller, è necessario digitarle nella finestra di dialogo **Accesso** che viene visualizzata.

Cambio tra utenti

Occorre essere collegati a SpamKiller in qualità di amministratore.

1. Fare clic su **Cambia utente** nella parte superiore della pagina. Viene visualizzata la finestra di dialogo **Cambia utente**.
2. Selezionare un utente, quindi fare clic su **OK**. Se l'utente dispone di una password, viene visualizzata la finestra di dialogo **Accesso**. Digitare la password utente nella casella **Password** e fare clic su **OK**.

Utilizzo dell'elenco degli amici

Si consiglia di aggiungere i nomi e gli indirizzi di posta elettronica dei propri amici all'elenco degli amici. SpamKiller non blocca i messaggi provenienti dagli utenti inclusi nell'elenco. L'aggiunta degli amici assicura, quindi, la ricezione dei messaggi autorizzati.

SpamKiller consente di aggiungere agli elenchi degli amici nomi, indirizzi di posta elettronica, domini e mailing list. È possibile aggiungere un indirizzo alla volta o tutti gli indirizzi contemporaneamente importando una rubrica dal programma di posta elettronica in uso.

SpamKiller gestisce due tipi di elenchi:

- **Elenco amici globale:** influisce su tutti gli account di posta elettronica per tutti gli utenti di SpamKiller. Se sono stati aggiunti più utenti, è necessario accedere a SpamKiller in qualità di amministratore per gestire questo elenco.
- **Elenco amici personali:** influisce su tutti gli account di posta elettronica associati a un utente specifico. Se sono stati aggiunti più utenti, è necessario accedere a SpamKiller in qualità di utente per gestire questo elenco.

È possibile aggiungere gli amici a un elenco per assicurarsi che i loro messaggi di posta elettronica non vengano bloccati. Nella pagina Amici vengono visualizzati i nomi e gli indirizzi aggiunti all'elenco degli amici, nonché la data in cui i nominativi sono stati aggiunti e il numero totale di messaggi ricevuti dagli stessi.

Fare clic sulla scheda **Indirizzi di e-mail** per visualizzare gli indirizzi di posta elettronica nell'elenco degli amici. Fare clic sulla scheda **Domini** per visualizzare gli indirizzi dei domini nell'elenco. Fare clic sulla scheda **Mailing list** per visualizzare le mailing list nell'elenco degli amici.

Per passare dall'elenco degli amici globale a quello degli amici personali, fare clic sulla freccia giù situata nella scheda **Indirizzi di e-mail**, **Domini** o **Mailing list**, quindi selezionare **Elenco amici personali**.

Apertura di un elenco degli amici

1 Per aprire un elenco degli amici, fare clic sulla scheda **Amici**. Viene visualizzata la pagina Amici (Figura 5-13).

2 Fare clic sulla scheda **Indirizzi di e-mail**, **Domini** o **Mailing list**. Viene visualizzato l'elenco degli amici globale. Per visualizzare l'elenco degli amici personali, fare clic sulla freccia giù in una delle schede, quindi selezionare **Elenco amici personali**.

NOTA
Se si utilizza Windows 2000 o Windows XP e sono stati aggiunti più utenti a SpamKiller, gli utenti con limitazioni possono visualizzare solo il proprio Elenco amici personali.

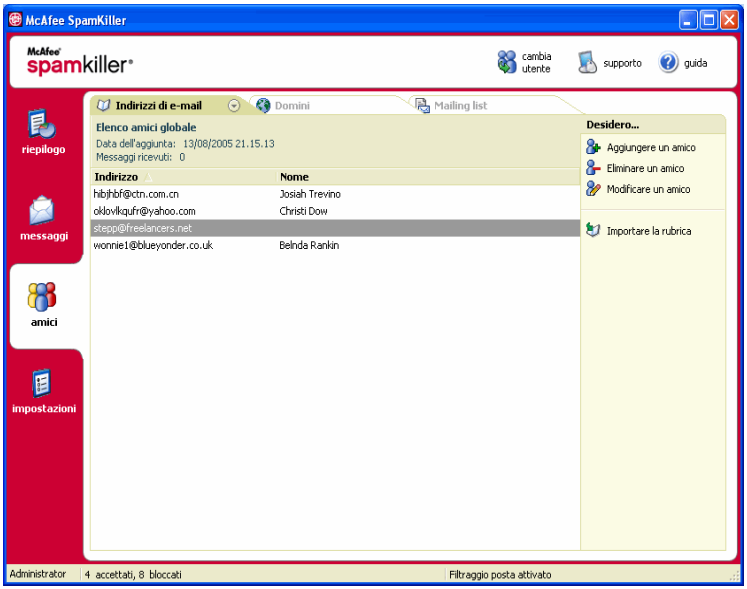


Figura 5-13. Pagina Amici

Importazione di rubriche

È possibile importare delle rubriche in un elenco degli amici manualmente o automaticamente. L'importazione automatica consente a SpamKiller di verificare regolarmente la presenza di nuovi indirizzi nelle rubriche e importarli automaticamente in un elenco degli amici.

È possibile importare delle rubriche dai seguenti programmi di posta elettronica:

- Microsoft Outlook 98 e versioni successive
- Microsoft Outlook Express (tutte le versioni)

- Netscape Communicator 6 e versioni precedenti (se le rubriche vengono esportate come file LDIF)
- Qualcomm Eudora 5 e versioni successive
- IncrediMail Xe
- MSN/Hotmail
- Tutti i programmi che consentono l'esportazione delle rubriche sotto forma di file di testo normale

Importazione automatica di una rubrica

È possibile aggiornare regolarmente l'elenco degli amici personali creando una pianificazione per l'importazione degli indirizzi dalle rubriche.

1. Fare clic sulla scheda **Impostazioni**, quindi su **Rubriche**. Viene visualizzata la finestra di dialogo **Importa rubriche**, in cui è presente un elenco di rubriche che SpamKiller verifica regolarmente e da cui importa i nuovi indirizzi.
2. Fare clic su **Aggiungi**. Viene visualizzata la finestra di dialogo **Importa pianificazione**.
3. Selezionare il **Tipo** di rubrica da importare e l'**Origine**.
4. Dalla casella **Pianificazione**, selezionare la frequenza con cui SpamKiller deve verificare la presenza di nuovi indirizzi nella rubrica.
5. Fare clic su **OK**. Al termine di un aggiornamento, i nuovi indirizzi sono visualizzati in Elenco amici personali.

Importazione manuale di una rubrica

È possibile importare manualmente delle rubriche nell'elenco degli amici personali o in quello degli amici globale.

> **NOTA**
> Se si utilizza Windows 2000 o Windows XP e sono stati aggiunti più utenti a SpamKiller, è necessario accedere al programma in qualità di amministratore per aggiungere gli amici all'elenco degli amici globale.

1. Fare clic sulla scheda **Amici**, quindi su **Importa rubrica**.

   Viene visualizzata la finestra di dialogo **Importa rubrica**, in cui viene visualizzato un elenco di tipi di rubriche che è possibile importare.
2. Selezionare il tipo di rubrica da importare o fare clic su **Sfoglia** per importare gli indirizzi memorizzati in un file.

Per importare la rubrica unicamente nell'elenco degli amici personali, verificare che la casella di controllo **Aggiungi a elenco amici personali** sia selezionata. Per importare la rubrica unicamente nell'elenco degli amici globale, verificare che la casella non sia selezionata.

3 Fare clic su **Avanti**. Il numero di indirizzi aggiunti viene elencato in una pagina di conferma.

4 Fare clic su **Fine**. Gli indirizzi vengono visualizzati in Elenco amici globale o in Elenco amici personali.

Modifica delle informazioni di una rubrica

È possibile modificare le informazioni di una rubrica importata automaticamente.

1 Fare clic sulla scheda **Impostazioni**, quindi su **Rubriche**.

2 Selezionare una rubrica, quindi fare clic su **Modifica**.

3 Modificare le informazioni sulla rubrica, quindi fare clic su **OK**.

Eliminazione di rubriche dall'elenco di importazione automatica

È possibile rimuovere una voce della rubrica quando non si desidera più che SpamKiller importi automaticamente gli indirizzi da tale rubrica.

1 Fare clic sulla scheda **Impostazioni**, quindi su **Rubriche**.

2 Selezionare la rubrica, quindi fare clic su **Elimina**. Viene visualizzata la finestra di dialogo di conferma.

3 Fare clic su **Sì** per rimuovere la rubrica dall'elenco.

Aggiunta di amici

Per assicurare la ricezione di tutti i messaggi di posta elettronica inviati dagli amici, aggiungerne i nomi e gli indirizzi a un elenco degli amici. È possibile aggiungere gli amici dalle pagine Amici, Posta bloccata e Posta accettata, nonché da Microsoft Outlook o Outlook Express.

NOTA
Se si utilizza Windows 2000 o Windows XP e sono stati aggiunti più utenti a SpamKiller, è necessario accedere al programma in qualità di amministratore per aggiungere gli amici all'elenco degli amici globale.

Aggiunta di amici dalla pagina Posta bloccata o Posta accettata

1. Fare clic sulla scheda **Messaggi**, quindi sulla scheda **Posta bloccata** o **Posta accettata**.

   Oppure

   Dal menu SpamKiller in Microsoft Outlook o Outlook Express, selezionare **Visualizza messaggi bloccati** per aprire la pagina Posta bloccata per l'account desiderato.

   Viene visualizzata la pagina Posta bloccata o Posta accettata.

2. Selezionare un messaggio proveniente da un mittente che si desidera aggiungere all'elenco degli amici, quindi fare clic su **Aggiungi un amico**.

3. Nella casella **Indirizzo**, digitare l'indirizzo da aggiungere all'elenco degli amici. È possibile che la casella **Indirizzo** contenga già l'indirizzo recuperato dal messaggio selezionato.

4. Digitare il nome dell'amico nella casella **Nome**.

5. Selezionare il tipo di indirizzo che si desidera aggiungere dalla casella **Tipo di amico**:

   - **Indirizzi di posta elettronica singoli:** l'indirizzo di posta elettronica del mittente viene aggiunto alla sezione Domini nell'elenco degli amici.
   - **Tutti nel dominio:** il nome del dominio viene aggiunto alla sezione **Domini** nell'elenco degli amici. Verranno accettati tutti i messaggi di posta elettronica provenienti dal dominio.
   - **Mailing list:** l'indirizzo viene aggiunto alla sezione **Mailing list** nell'elenco degli amici.

   Per aggiungere l'indirizzo unicamente all'elenco degli amici personali, verificare che la casella di controllo **Aggiungi a elenco amici personali** sia selezionata. Per aggiungere l'indirizzo unicamente all'elenco degli amici globale, verificare che la casella non sia selezionata.

6. Fare clic su **OK**. Tutti i messaggi provenienti da quell'amico vengono contrassegnati come messaggi inviati da un amico e visualizzati nella pagina Posta accettata.

Aggiunta di amici dalla pagina Amici

1. Fare clic sulla scheda **Amici**, quindi su **Aggiungi un amico**. Viene visualizzata la finestra di dialogo **Proprietà amico**.

2. Nella casella **Indirizzo**, digitare l'indirizzo da aggiungere all'elenco degli amici.

3. Digitare il nome dell'amico nella casella **Nome**.

4 Selezionare il tipo di indirizzo che si desidera aggiungere dalla casella **Tipo di amico**:

- **Indirizzi di posta elettronica singoli:** l'indirizzo di posta elettronica del mittente viene aggiunto alla sezione Domini nell'elenco degli amici.
- **Tutti nel dominio:** il nome del dominio viene aggiunto alla sezione **Domini** nell'elenco degli amici. Verranno accettati tutti i messaggi di posta elettronica provenienti dal dominio.
- **Mailing list:** l'indirizzo viene aggiunto alla sezione **Mailing list** nell'elenco degli amici.

Per aggiungere l'indirizzo unicamente all'elenco degli amici personali, verificare che la casella di controllo **Aggiungi a elenco amici personali** sia selezionata. Per aggiungere l'indirizzo unicamente all'elenco degli amici globale, verificare che la casella non sia selezionata.

5 Fare clic su **OK**. Tutti i messaggi provenienti da quell'amico vengono contrassegnati come messaggi inviati da un amico e visualizzati nella pagina Posta accettata.

Aggiunta di amici da Microsoft Outlook

1 Aprire il proprio account di posta elettronica in Microsoft Outlook o Outlook Express.

2 Selezionare un messaggio proveniente da un mittente che si desidera aggiungere all'elenco degli amici.

3 Fare clic su nella barra delle applicazioni di Microsoft Outlook. Tutti i messaggi provenienti da quell'amico vengono contrassegnati come messaggi inviati da un amico e visualizzati nella pagina Posta accettata.

Modifica di amici

1 Fare clic sulla scheda **Amici**, quindi sulla scheda **Indirizzi di e-mail**, **Domini** o **Mailing list**.

Viene visualizzato l'elenco degli amici globale. Per visualizzare l'elenco degli amici personali, fare clic sulla freccia giù in una delle schede, quindi selezionare **Elenco amici personali**.

> **NOTA**
> Se si utilizza Windows 2000 o Windows XP e sono stati aggiunti più utenti a SpamKiller, solo gli amministratori possono accedere all'elenco degli amici globale.

2 Selezionare un indirizzo dall'elenco, quindi scegliere **Modifica**.

3 Modificare le informazioni appropriate, quindi fare clic su **OK**.

Eliminazione di amici

È possibile rimuovere da un elenco degli amici gli indirizzi non più utilizzati.

1 Fare clic sulla scheda **Amici**, quindi sulla scheda **Indirizzi di e-mail**, **Domini** o **Mailing list**.

Viene visualizzato l'elenco degli amici globale. Per visualizzare l'elenco degli amici personali, fare clic sulla freccia giù in una delle schede, quindi selezionare **Elenco amici personali**.

NOTA
Se si utilizza Windows 2000 o Windows XP e sono stati aggiunti più utenti a SpamKiller, solo gli amministratori possono accedere all'elenco degli amici globale.

2 Selezionare un indirizzo dall'elenco, quindi scegliere **Elimina amico**. Viene visualizzata una finestra di dialogo di conferma.

3 Fare clic su **Sì** per eliminare l'amico.

Utilizzo dei messaggi bloccati e accettati

Fare clic sulla scheda **Messaggi** per aprire la pagina Messaggi (Figura 5-14) e accedere ai messaggi bloccati e accettati. Le pagine Posta bloccata e Posta accettata hanno funzioni simili.

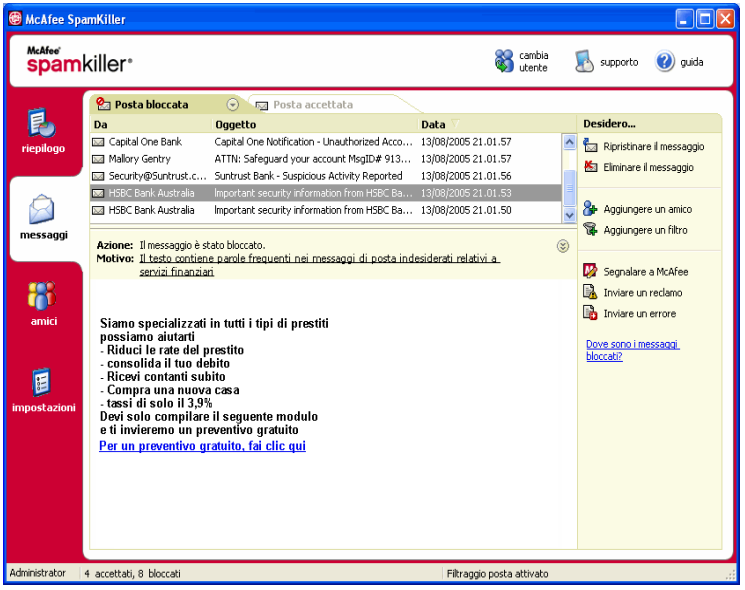


Figura 5-14. Pagina Messaggi

Pagina Posta bloccata

Fare clic sulla scheda **Posta bloccata** nella pagina Messaggi per visualizzare i messaggi bloccati.

> **NOTA**
> È possibile accedere ai messaggi bloccati anche in Microsoft Outlook selezionando il menu SpamKiller e facendo clic su **Visualizza messaggi bloccati**.

I messaggi bloccati sono messaggi che SpamKiller ha identificato come messaggi indesiderati, rimosso dalla cartella Posta in arrivo e collocato nella pagina Posta bloccata.

Nella pagina Posta bloccata vengono visualizzati tutti i messaggi di posta indesiderati rimossi dagli account di posta elettronica. Per visualizzare i messaggi bloccati per un account specifico, fare clic sulla freccia giù situata nella scheda **Posta bloccata**, quindi selezionare l'account da visualizzare.

Nel riquadro superiore dei messaggi vengono elencati i messaggi indesiderati ordinati per data. Il messaggio più recente viene visualizzato per primo. Il riquadro inferiore di anteprima contiene il testo del messaggio selezionato.

> **NOTA**
> Se si utilizza Windows 2000 o Windows XP, se sono stati aggiunti più utenti a SpamKiller e se si è connessi come utenti con limitazioni, il contenuto del messaggio non viene visualizzato nel riquadro di anteprima inferiore.

Il riquadro centrale mostra i dettagli dei messaggi. Fare clic sulle frecce giù per espandere il riquadro dei dettagli e visualizzare il testo e le intestazioni in formato nativo, compresi eventuali tag HTML di formattazione. Il riquadro dei dettagli dei messaggi contiene le opzioni seguenti.

- **Azione:** descrive la modalità di elaborazione del messaggio indesiderato. Azione è associata all'azione del filtro che ha bloccato il messaggio.
- **Motivo:** spiega il motivo per cui è stato bloccato il messaggio. È possibile fare clic sul motivo per aprire l'editor dei filtri e visualizzare il filtro. Nell'editor dei filtri vengono visualizzati l'aspetto del filtro in un messaggio e l'azione intrapresa da SpamKiller nei confronti dei messaggi individuati dal filtro.
- **Da:** visualizza il mittente del messaggio.
- **Data:** visualizza la data di invio del messaggio.
- **A:** visualizza il destinatario del messaggio.
- **Oggetto:** mostra l'argomento visualizzato alla riga del messaggio relativa all'oggetto.

Se sono stati inviati messaggi di errore o reclami manuali, la colonna di sinistra contiene le relative icone accanto ai messaggi.

- Inviato reclamo : è stato inviato un reclamo relativo al messaggio.
- Inviato messaggio di errore : è stato inviato un messaggio di errore all'indirizzo di risposta del messaggio indesiderato.
- Inviati reclamo e messaggio di errore : sono stati inviati sia un reclamo che un messaggio di errore.

Per ulteriori informazioni sui messaggi bloccati, vedere *Dove sono i messaggi bloccati* a pagina 125.

Pagina Posta accettata

Fare clic sulla scheda **Posta accettata** nella pagina Messaggi per visualizzare i messaggi accettati.

Nella pagina Posta accettata vengono visualizzati tutti i messaggi presenti nella cartella Posta in arrivo di tutti gli account di posta elettronica. Per gli account MAPI, la pagina Posta accettata non contiene i messaggi interni. Per visualizzare i messaggi accettati per un account specifico, fare clic sulla freccia giù situata nella scheda **Posta accettata**, quindi selezionare l'account da visualizzare.

> **NOTA**
> SpamKiller è progettato per accettare i messaggi autorizzati. Tuttavia, se i messaggi autorizzati vengono visualizzati nell'elenco Posta bloccata, è possibile spostarli nella cartella Posta in arrivo e nell'elenco Posta accettata, selezionandoli e facendo clic su **Ripristina messaggio**.

Come nella pagina Posta bloccata, il riquadro superiore mostra i messaggi ordinati per data. Il riquadro inferiore di anteprima contiene il testo del messaggio selezionato.

Il riquadro centrale indica se un messaggio è stato inviato da un utente incluso nell'elenco degli amici o se soddisfa i criteri di un filtro, ma l'azione del filtro è stata impostata su **Accetta** o **Contrassegna come possibile spam**. Fare clic sulle frecce giù per espandere il riquadro dei dettagli e visualizzare il testo e le intestazioni del messaggio in formato nativo, compresi eventuali tag HTML.

Il riquadro dei dettagli dei messaggi contiene le opzioni seguenti.

- **Azione:** descrive la modalità di elaborazione del messaggio.
- **Motivo:** se un messaggio è stato contrassegnato da SpamKiller, questo campo ne spiega la ragione.
- **Da:** visualizza il mittente del messaggio.

- **Data:** visualizza la data di invio del messaggio.
- **A:** visualizza il destinatario del messaggio.
- **Oggetto:** mostra l'argomento visualizzato alla riga del messaggio relativa all'oggetto.

Accanto ai messaggi viene visualizzata una delle seguenti icone.

- Messaggio di posta elettronica inviato da un amico : SpamKiller rileva che il mittente del messaggio è incluso in un elenco degli amici. Questo messaggio viene conservato.
- Possibile messaggio indesiderato : il messaggio corrisponde a un filtro con un'azione impostata su Contrassegna come possibile spam.
- Inviato reclamo : è stato inviato un reclamo relativo al messaggio.
- Inviato messaggio di errore : è stato inviato un messaggio di errore all'indirizzo di risposta del messaggio indesiderato.
- Inviati reclamo e messaggio di errore : sono stati inviati sia un reclamo che un messaggio di errore.

Operazioni relative alla posta bloccata e accettata

Nel riquadro destro delle pagine Posta bloccata e Posta accettata vengono elencate le operazioni eseguibili.

- **Blocca messaggio:** rimuove il messaggio dalla cartella Posta in arrivo e lo colloca nella pagina Posta bloccata di SpamKiller (questa opzione è visualizzata solo nella pagina Posta accettata).
- **Ripristina messaggio:** ricolloca il messaggio nella cartella Posta in arrivo (questa opzione è visualizzata solo nella pagina Posta bloccata) e apre la finestra di dialogo **Opzioni di ripristino**. È possibile aggiungere automaticamente il mittente all'elenco degli amici e ripristinare tutti i messaggi inviati dal mittente.
- **Elimina messaggio:** rimuove il messaggio selezionato.
- **Aggiungi un amico:** aggiunge a un elenco degli amici il nome, l'indirizzo di posta elettronica e il dominio del mittente o di una mailing list.
- **Aggiungi un filtro:** crea un filtro.
- **Segnala a McAfee:** informa McAfee riguardo a specifici messaggi indesiderati ricevuti.

- **Invia un reclamo:** invia un reclamo relativo al messaggio indesiderato all'amministratore del dominio del mittente o a un altro indirizzo di posta elettronica specificato.
- **Invia un errore:** invia un messaggio di errore all'indirizzo di risposta di un messaggio indesiderato.

Ripristino di messaggi

Se la pagina Posta bloccata o la cartella SpamKiller in Microsoft Outlook e Outlook Express contengono messaggi autorizzati, è possibile ricollocare tali messaggi nella cartella Posta in arrivo.

Dalla pagina Posta bloccata

1. Fare clic sulla scheda **Messaggi**, quindi sulla scheda **Posta bloccata**.

   Oppure

   Dal menu SpamKiller in Microsoft Outlook o Outlook Express, selezionare **Visualizza messaggi bloccati** per aprire la pagina Posta bloccata per l'account desiderato.

2. Selezionare un messaggio e scegliere **Ripristina messaggio** . Verrà visualizzata la finestra di dialogo **Opzioni di ripristino**.

   - **Aggiungi amico:** aggiunge il mittente all'elenco degli amici.
   - **Ripristina tutti dallo stesso mittente:** ripristina tutti i messaggi bloccati inviati dal mittente del messaggio selezionato.

3. Fare clic su **OK**. Il messaggio viene spostato nella cartella Posta in arrivo e nella pagina Posta accettata.

Dalla cartella SpamKiller in Microsoft Outlook o da Outlook Express

Selezionare i messaggi desiderati e fare clic su **Ripristina selezione** dal menu o dalla barra degli strumenti di SpamKiller. I messaggi selezionati vengono spostati nella cartella Posta in arrivo e il tag [SPAM] (predefinito) viene rimosso.

Blocco di messaggi

È possibile bloccare i messaggi indesiderati presenti nella cartella Posta in arrivo. Quando si blocca un messaggio, SpamKiller crea automaticamente un filtro per rimuovere il messaggio dalla cartella Posta in arrivo. È possibile bloccare i messaggi presenti nella cartella Posta in arrivo dalla pagina Posta accettata, da Microsoft Outlook o da Outlook Express.

Dalla pagina Posta accettata

1. Fare clic sulla scheda **Messaggi**, quindi sulla scheda **Posta accettata**. Viene visualizzata la pagina Posta accettata con i messaggi presenti nella cartella Posta in arrivo.
2. Selezionare un messaggio, quindi fare clic su **Blocca messaggio**. Il messaggio viene rimosso dalla cartella Posta in arrivo e dalla pagina Posta accettata, mentre una copia del messaggio viene visualizzata nella pagina Posta bloccata.

Da Microsoft Outlook

In Microsoft Outlook, i messaggi provenienti dai membri di un server Exchange sono considerati sicuri e non vengono filtrati con SpamKiller. Vengono filtrati soltanto i messaggi provenienti da fonti esterne.

1. Aprire la cartella Posta in arrivo di Microsoft Outlook o Outlook Express.
2. Selezionare un messaggio, quindi fare clic su . Una copia del messaggio viene collocata nella pagina Posta bloccata.

Dove sono i messaggi bloccati

Per impostazione predefinita, i messaggi indesiderati vengono contrassegnati con il tag [SPAM] e spostati nella cartella SpamKiller di Outlook e Outlook Express oppure in Posta in arrivo. I messaggi contrassegnati vengono visualizzati anche nella pagina Posta accettata.

Eliminazione manuale di un messaggio

1. Fare clic sulla scheda **Messaggi**, quindi sulla scheda **Posta bloccata**.

   Oppure

   Dal menu SpamKiller in Microsoft Outlook o Outlook Express, selezionare **Visualizza messaggi bloccati** per aprire la pagina Posta bloccata per l'account desiderato.

2. Selezionare un messaggio da eliminare.

3. Fare clic su **Elimina messaggio**. Viene visualizzata la finestra di dialogo di conferma.

4. Fare clic su **Sì** per eliminare il messaggio.

Modifica della modalità di elaborazione dei messaggi indesiderati

Quando viene rilevato, il messaggio indesiderato viene contrassegnato o bloccato. I messaggi indesiderati vengono rimossi dal server ogni volta che SpamKiller si collega ad esso.

Assegnazione di contrassegni

L'oggetto del messaggio di posta elettronica viene contrassegnato con il tag [SPAM], il messaggio viene conservato nella cartella Porta in arrivo o nella cartella SpamKiller, se si sta utilizzando Microsoft Outlook o Outlook Express.

Blocco

Il messaggio viene rimosso e collocato nella pagina Posta bloccata di SpamKiller. È possibile ripristinare i messaggi autorizzati eventualmente bloccati (vedere la sezione Ripristino di messaggi).

SpamKiller elimina automaticamente i messaggi bloccati dalla pagina Posta bloccata dopo 15 giorni. È possibile modificare la frequenza con cui vengono rimossi i messaggi bloccati.

SpamKiller non rimuove automaticamente i messaggi dalla pagina Posta accettata poiché quest'ultima contiene i messaggi presenti nella cartella Posta in arrivo.

Modifica della modalità di elaborazione dei messaggi indesiderati

1. Fare clic sulla scheda **Impostazioni**, quindi sull'icona **Opzioni di filtraggio**.
2. Fare clic sulla scheda **Elaborazione**.
   - **Colloca messaggi di posta indesiderati nella casella Posta bloccata:** i messaggi indesiderati vengono rimossi dalla cartella Posta in arrivo e collocati nella pagina Posta bloccata di SpamKiller.
   - **Identifica messaggio indesiderato e conserva in Posta in arrivo:** impostazione predefinita. I messaggi indesiderati restano nella cartella Posta in arrivo e la riga dell'oggetto include il tag [SPAM].

     Conserva posta bloccata per ____ giorni: i messaggi bloccati restano nella pagina Posta bloccata per il periodo specificato.

     Conserva posta accettata per ____ giorni: i messaggi accettati restano nella pagina Posta accettata per il periodo specificato.
3. Fare clic su **OK**.

Utilizzo di AntiPhishing Filter

I messaggi non richiesti vengono classificati come indesiderati (messaggi che invitano all'acquisto) o come phishing (messaggi che richiedono il rilascio di informazioni personali a siti Web ingannevoli o potenzialmente ingannevoli).

McAfee AntiPhishing Filter consente la protezione dai siti Web in blacklist (per i siti ingannevoli o la cui attività di phishing è confermata) o in graylist (per i siti con contenuti pericolosi o collegamenti a siti Web presenti nella blacklist).

Se si visita un sito Web ingannevole o potenzialmente ingannevole, si viene reindirizzati alla pagina di McAfee AntiPhishing Filter.

Per modificare le impostazioni di AntiPhishing, attenersi alla seguente procedura:

1. Aprire Internet Explorer.
2. Dal menu **Strumenti**, selezionare **McAfee AntiPhishing Filter**.

- **Attiva filtro siti Web:** casella di controllo attivata per impostazione predefinita. Per disattivare AntiPhishing Filter, deselezionare la casella di controllo.
- **Autorizza accesso ai siti Web in blacklist:** inserisce un collegamento sulla pagina di reindirizzamento per i siti in blacklist. Facendo clic su tale collegamento è possibile visitare il relativo sito Web.
- **Autorizza accesso ai siti Web in graylist:** inserisce un collegamento sulla pagina di reindirizzamento per i siti in graylist. Facendo clic su tale collegamento è possibile visitare il relativo sito Web.

3. Al termine dell'operazione, fare clic su **OK**.

Aggiunta di amici a un elenco degli amici

Vedere la sezione *Aggiunta di amici dalla pagina Posta bloccata o Posta accettata* a pagina 118.

Aggiunta di filtri

Per ulteriori informazioni sui filtri, vedere la sezione *Utilizzo dei filtri* nella Guida in linea.

1. Per creare un filtro globale, fare clic sulla scheda **Impostazioni**, selezionare **Filtri globali** e fare clic su **Aggiungi**.

   Oppure

   Per creare un filtro personale, fare clic sulla scheda **Impostazioni**, selezionare **Filtri personali** e fare clic su **Aggiungi**.

   Oppure

   Fare clic sulla scheda **Messaggi**, quindi sulla scheda **Posta bloccata** o **Posta accettata**, infine su **Aggiungi un filtro**.

2. Fare clic su **Aggiungi** per creare una condizione del filtro. Viene visualizzata la finestra di dialogo **Condizione filtro**.

3. Creare una condizione del filtro attenendosi a questi passaggi.

   Una condizione del filtro è un'istruzione che indica a SpamKiller cosa cercare in un messaggio. Nell'esempio "Il testo del messaggio contiene mutuo", il filtro cerca i messaggi il cui testo contiene la parola "mutuo". Per ulteriori informazioni, vedere *Condizioni del filtro* nella Guida in linea.

   a. Selezionare un tipo di condizione dalla prima casella.

   b. Selezionare o immettere dei valori nelle caselle successive.

   c. Se vengono visualizzate le opzioni riportate di seguito, selezionarle per definire ulteriormente la condizione del filtro.

      Cerca anche nei codici di formattazione: questa opzione viene visualizzata solo se la condizione del filtro è definita per la ricerca del testo del messaggio. Se si seleziona la casella di controllo, SpamKiller cerca sia il testo che i codici di formattazione del messaggio per il testo indicato.

      Variazioni di corrispondenza: consente a SpamKiller di rilevare errori di ortografia comuni e intenzionali utilizzati dai mittenti dei messaggi indesiderati. Ad esempio, la parola "comune" potrebbe essere scritta "c0mun3" per eludere i filtri.

Espressioni regolari (RegEx): consente di specificare le sequenze di caratteri nelle condizioni del filtro. Per provare una sequenza di caratteri, fare clic su **Prova RegEx**.

Maiuscole/minuscole: questa opzione viene visualizzata solo per le condizioni in cui è stato specificato un valore. Se si seleziona la casella di controllo, SpamKiller distingue le lettere maiuscole e minuscole nel valore specificato.

d Fare clic su **OK**.

4 Creare un'altra condizione del filtro come indicato di seguito o andare al Passaggio 5 per selezionare un'azione del filtro.

a Fare clic su **Aggiungi**, quindi creare una condizione del filtro. Fare clic su **OK** al termine della creazione della condizione del filtro.

Entrambe le condizioni del filtro sono incluse nell'elenco Condizioni filtro e sono unite da **e**, che indica a SpamKiller di cercare i messaggi che soddisfano *entrambe* le condizioni del filtro. Se si desidera che SpamKiller cerchi i messaggi corrispondenti a una delle condizioni, sostituire **e** con **o** facendo clic su **e**, quindi selezionando **o** dalla casella visualizzata.

b Fare clic su **Aggiungi** per creare un'altra condizione del filtro o andare al Passaggio 5 per selezionare un'azione del filtro.

Se si creano tre o più condizioni del filtro, è possibile raggrupparle per creare delle clausole. Per gli esempi di raggruppamento, vedere la sezione *Raggruppamento di filtri* nella Guida in linea.

Per raggruppare le condizioni del filtro, selezionare una condizione del filtro, quindi fare clic su **Raggruppa**. Per separare le condizioni del filtro, selezionare una condizione raggruppata, quindi fare clic su **Separa**.

5 Selezionare un'azione del filtro dalla casella **Azione**. L'azione del filtro indica a SpamKiller come elaborare i messaggi individuati dal filtro. Per ulteriori informazioni, vedere la sezione *Azioni del filtro* nella Guida in linea.

6 Fare clic su **Avanzate** per selezionare le opzioni di filtraggio avanzate. La selezione delle opzioni avanzate non è obbligatoria. Per ulteriori informazioni, vedere la sezione *Opzioni di filtraggio avanzate* nella Guida in linea.

7 Fare clic su **OK** al termine della creazione del filtro.

NOTA
Per modificare una condizione, selezionarla e fare clic su **Modifica**. Per eliminare una condizione, selezionarla e fare clic su **Elimina**.

Espressioni regolari (RegEx)

Le espressioni regolari sono disponibili soltanto per le seguenti condizioni del filtro: **L'oggetto**, **Il testo del messaggio**, **Almeno una delle frasi che seguono**.

I caratteri speciali e le sequenze possono essere utilizzati come espressioni regolari nella definizione delle condizioni del filtro. Ad esempio:

- L'espressione regolare **[0-9]*\,[0-9]+** indica i numeri decimali fluttuanti senza annotazioni tecniche. L'espressione regolare indica: “12,12”, “,1212” e “12,0”, ma non “12” e “12”.
- L'espressione regolare **\D*[0-9]+\D*** indica tutte le parole con numeri: “SpamKi11er” e “V1AGRA”, ma non “SpamKiller” e “VIAGRA”.

****

Indica il carattere successivo sia sotto forma di carattere speciale, sia sotto forma di carattere letterale. Ad esempio, “n” indica il carattere “n”. “\n” indica il carattere di nuova riga. La sequenza “\\” indica “\” e “\(” indica “(”.

^

Indica l'inizio dell'immissione.

$

Indica la fine dell'immissione.

*****

Annulla il carattere precedente o ne indica la ripetizione. Ad esempio, “zo*” indica “z” o “zoo”.

+

Indica il carattere precedente una o più volte. Ad esempio, “zo+” indica “zoo”, ma non “z”.

?

Annulla il carattere precedente o lo indica una volta. Ad esempio, “a?ve?” indica il carattere “ve” in “neve”.

.

Indica qualsiasi carattere singolo tranne il carattere di nuova riga.

(sequenza)

Indica la sequenza e ricorda la corrispondenza. La sottostringa corrispondente può essere recuperata dalla raccolta di corrispondenze ottenuta, utilizzando Elemento [0]...[n]. Per indicare i caratteri di parentesi ( ), utilizzare “\(“ o ”\)”.

x|y

Indica x o y. Ad esempio, “z|igloo” indica “z” o “igloo”. “(z|igl)oo” indica “zoo” o “igloo”.

{n}

n indica un numero intero non negativo. Indica esattamente n volte. Ad esempio, “s{2}” non indica la “s” in “asilo”, ma le prime due “s” in “cassssse”.

{n,}

n indica un numero intero non negativo. Indica almeno n volte. Ad esempio, “s{2,}” non indica la “s” in “asilo”, ma tutte le “s” in “cassssse”; .“s{1,}” equivale a “s+”. “s{0,}” equivale a “s*”.

{n,m}

m ed n indicano numeri interi non negativi. Indicano almeno n volte e al massimo m volte. Ad esempio, “s{1,3}” indica le prime tre “s” in “cassssse”; .“s{0,1,}” equivale a “s?”.

[xyz]

Un set di caratteri. Indica qualsiasi carattere tra quelli inclusi. Ad esempio, “[abc]” indica la “a” in “piano”.

[^xyz]

Un set di caratteri negativo. Indica qualsiasi carattere tra quelli non inclusi. Ad esempio, “[^abc]” indica la “o” in “baco”.

[a-z]

Un intervallo di caratteri. Indica qualsiasi carattere nell'intervallo specificato. Ad esempio, “[a-z]” indica qualsiasi carattere minuscolo nell'intervallo tra “a” e “z”.

[^m-z]

Un intervallo di caratteri negativo. Indica qualsiasi carattere non nell'intervallo specificato. Ad esempio, “[m-z]” indica qualsiasi carattere minuscolo non nell'intervallo tra “m” e “z”.

\b

Indica il limite di una parola, ovvero la posizione tra la parola e uno spazio. Ad esempio, “ve\b” indica “ve” in “neve”, ma non indica “ve” in “evento”.

\B

Indica l'assenza di limite della parola. “do*p\B” indica “dop” in “subito dopo”.

\d

Indica un numero. Equivale a [0-9].

\D

Indica un carattere che non è un numero. Equivale a [^0-9].

\f

Indica un carattere di modulo continuo.

\n

Indica il carattere di nuova riga.

\r

Indica il carattere di ritorno a capo.

\s

Indica qualsiasi spazio bianco tra cui spazio, tabulazione, modulo continuo e così via. Equivale a "[\f\n\r\t\v]".

\S

Indica qualsiasi carattere diverso dallo spazio. Equivale a "[^ \f\n\r\t\v]".

\t

Indica un carattere di tabulazione.

\v

Indica un carattere di tabulazione verticale.

\w

Indica qualsiasi parola che include un carattere di sottolineatura. Equivale a "[A-Za-z0-9_]".

\W

Indica qualsiasi carattere che non è una parola. Equivale a "[^A-Za-z0-9_]".

\num

Indica num, dove num è un numero intero positivo. Rappresenta un riferimento alle corrispondenze ricordate. Ad esempio, "(.)\1" indica due caratteri consecutivi identici.

\n

Indica n, quando n è un valore di escape ottale. I valori di escape ottale devono essere di 1, 2 o 3 cifre. Ad esempio, "\11" e "\011" indicano un carattere di tabulazione. "\0011" equivale a "\001" e "1". I valori di escape ottale non possono superare il valore 256. Se lo superano, soltanto le prime due cifre verranno considerate nell'espressione. Consente l'utilizzo dei codici ASCII nelle espressioni regolari.

\xn

Indica n, quando n è un valore di escape esadecimale. I valori di escape esadecimale devono essere esattamente di 2 cifre. Ad esempio, "\x41" indica "A". "\x041" equivale a "\x04" e "1". Consente l'utilizzo dei codici ASCII nelle espressioni regolari.

Segnalazione dei messaggi indesiderati a McAfee

È possibile segnalare i messaggi indesiderati a McAfee, che li analizzerà per creare aggiornamenti dei filtri.

1. Fare clic sulla scheda **Messaggi**, quindi sulla scheda **Posta bloccata** o **Posta accettata**. Viene visualizzata la pagina Posta bloccata o Posta accettata.
2. Selezionare un messaggio, quindi fare clic su **Segnala a McAfee**. Viene visualizzata la finestra di dialogo di conferma.
3. Fare clic su **Sì**. Il messaggio viene inviato automaticamente a McAfee.

Invio manuale di reclami

È possibile inviare un reclamo per impedire la ricezione di ulteriori messaggi indesiderati da parte di un mittente. Per ulteriori informazioni sull'invio di reclami, vedere la sezione *Invio di reclami e messaggi di errore* nella Guida in linea.

1. Fare clic sulla scheda **Messaggi**, quindi sulla scheda **Posta bloccata** o **Posta accettata**. Verrà visualizzato un elenco di messaggi.
2. Selezionare il messaggio per cui inviare un reclamo, quindi scegliere **Invia reclamo**. Viene visualizzata la finestra di dialogo **Invia reclamo**.
3. Selezionare il destinatario del reclamo.

   ATTENZIONE
   In molti casi non è necessario selezionare **Mittente**. L'invio di un reclamo al mittente convalida il proprio indirizzo di posta elettronica e potrebbe causare un aumento del numero di messaggi indesiderati inviati dallo stesso mittente.
4. Fare clic su **Avanti**, quindi attenersi alle istruzioni contenute nelle finestre di dialogo visualizzate.

Invio di messaggi di errore

Per ulteriori informazioni sull'invio di messaggi di errore, vedere la sezione *Invio di reclami e messaggi di errore* nella Guida in linea.

È possibile inviare un messaggio di errore per impedire la ricezione di ulteriori messaggi indesiderati da parte di un mittente.

Invio manuale di un messaggio di errore:

1. Fare clic sulla scheda **Messaggi**, quindi sulla scheda **Posta bloccata** o **Posta accettata**. Verrà visualizzato un elenco di messaggi.
2. Per selezionare un messaggio di errore relativo a un messaggio indesiderato specifico, selezionare il messaggio, quindi fare clic su **Invia errore**. Un messaggio di errore viene inviato all'indirizzo di risposta del messaggio indesiderato.

Indice

A

accesso a SpamKiller in un ambiente multiutente, 113
account di posta elettronica, 103
  aggiunta, 103
  eliminazione, 104
  indicare a SpamKiller il client di posta elettronica, 104
  modifica, 105
  modifica di account MAPI, 109
  modifica di account MSN/Hotmail, 107
  modifica di account POP3, 105
ActiveShield
  attivazione, 19
  avvio, 21
  disattivazione, 20
  impostazione di scansione predefinita, 21, 24 to 28
  interruzione, 21
  opzioni di scansione, 20
  pulizia di un virus, 29
  ricerca di nuovi virus sconosciuti, 27
  ricerca di script, 27
  ricerca di worm, 24
  scansione degli allegati di messaggi immediati in ingresso, 25
  scansione di messaggi di posta elettronica e allegati, 22
  scansione di tutti i file, 26
  scansione di tutti i tipi di file, 26
  scansione esclusivamente di file di programma e documenti, 26
  scansione per la ricerca di programmi potenzialmente indesiderati (PUP), 28
  verifica, 17
Aggiornamenti automatici di Windows, 73
aggiornamento
  disco di ripristino, 44
  VirusScan
    automatico, 47
    manuale, 47
aggiunta di account di posta elettronica, 103
aggiunta di filtri, 128
aggiunta di un indirizzo a un elenco degli amici, 117
aggiunta di utenti, 84
  blocco dei cookie, 85
  blocco di contenuto, 84
  limitazioni orari di accesso a Internet, 85
allegati dei messaggi immediati in ingresso
  pulizia automatica, 25
  scansione, 25
amministratore, 81, 110, 112
  recupero della password, 82
applicazioni Internet
  autorizzazione e blocco, 61
  informazioni, 59
  modifica regole applicazioni, 60
assistente di installazione, 82
AVERT, invio dei file sospetti, 42
avvisi
  Applicazione Internet bloccata, 72
  file infetti, 30
  L'applicazione è stata modificata, 73
  L'applicazione richiede l'accesso a Internet, 72
  L'applicazione richiede l'Accesso server, 73
  messaggi di posta elettronica infetti, 30
  Nuova applicazione autorizzata, 78
  potenziali worm, 31
  PUP, 31
  script sospetti, 30
  Tentativo di connessione bloccato, 79
  virus, 29

B

blocco di messaggi, 125

C

cambio di utente, 113
cavalli di Troia
  avvisi, 29
  rilevamento, 39
configurazione
  VirusScan
    ActiveShield, 19
    Scansione, 33
creazione di un disco di ripristino, 42

D

disco di ripristino
  aggiornamento, 44
  creazione, 42
  protezione da scrittura, 43
  utilizzo, 40, 44
disinstallazione
  altri firewall, 51

E

elenco degli amici, 114
  aggiunta di amici dalla pagina Posta bloccata o Posta accettata, 118
  aggiunta di un indirizzo di posta elettronica, 117
  importazione di una rubrica, 115
elenco dei file rilevati (funzione di scansione), 36, 39
Elenco PUP affidabili, 32
Esplora risorse, 36
espressioni regolari, 130
eventi
  archiviazione del Registro eventi, 70
  cancellazione del Registro eventi, 71
  copia, 71
  da 0.0.0.0, 62
  da 127.0.0.1, 63
  da indirizzi IP privati, 64
  dai computer nella LAN, 63
  eliminazione, 72
  esportazione, 71
  informazioni, 61
  loopback, 63
  risposta, 66
  segnalazione, 67
  suggerimenti da HackerWatch.org, 67
  traccia
    informazioni, 61
    visualizzazione dei registri degli eventi archiviati, 71
  ulteriori informazioni, 67
  visualizzazione
    con le stesse informazioni sull'evento, 66
    da un indirizzo, 66
    del giorno selezionato, 65
    della settimana, 65
    odierni, 65
    tutti, 65

F

filtraggio
  attivazione, 101
  disattivazione, 101
filtri, aggiunta, 128
firewall predefinito, impostazione, 51
funzioni, 81, 99

H

HackerWatch.org
  registrazione, 67
  segnalazione di un evento, 67
  suggerimenti, 67

I

icona Cambia utente, 100
icona Guida in linea, 101
icona Supporto, 101
importazione di una rubrica in un elenco degli amici, 115
indicare a SpamKiller il client di posta elettronica, 104
indirizzi IP
  affidabilità, 68
  esclusione, 69
  informazioni, 62
invio dei file sospetti ad AVERT, 42

M

McAfee Privacy Service, 83
accesso, 83
aggiornamento, 84
apertura, 83
disattivazione, 83
McAfee SecurityCenter, 13
messaggi di posta elettronica e allegati
pulizia automatica
attivazione, 22
scansione
attivazione, 22
disattivazione, 23
errori, 23
Microsoft Outlook, 37
modifica di utenti, 86
blocco dei cookie, 87
gruppo di età, 88
informazioni di un utente, 86
limitazioni orari di accesso a Internet, 88
password, 86
rimozione di utenti, 89
utente di avvio, 89
modifica di whitelist, 32

N

nuove funzioni, 15, 49

O

operazioni per messaggi bloccati e accettati, 123
opzione Analizza contenuto dei file compressi (funzione di scansione), 34
opzione Analizza sottocartelle (funzione di scansione), 34
opzione Analizza tutti i file (funzione di scansione), 34
opzione Ricerca nuovi virus sconosciuti (funzione di scansione), 35
opzione Ricerca programmi potenzialmente indesiderati (funzione di scansione), 35
opzioni, 89
autorizzazione di cookie, 92
autorizzazione di siti Web, 90
backup, 95
blocco di informazioni, 90
blocco di pubblicità, 91
blocco di siti Web, 89
Web bug, 91
opzioni di scansione
ActiveShield, 20, 26
Scansione, 33
opzioni utente, 96
accettazione di cookie, 98
cancellazione della cache, 97
modifica del nome utente, 97
modifica della password, 97
rifiuto di cookie, 98

P

pagina Amici, 115
pagina Impostazioni, 103
pagina Messaggi, 120
pagina Posta accettata, 122
pagina Posta bloccata, 121
pagina Riepilogo, 54, 101
password, 112
Personal Firewall
verifica, 54
pianificazione delle scansioni, 37
Posta accettata
aggiunta all'elenco degli amici, 128
icone nell'elenco messaggi accettati, 123
invio di messaggi di errore, 134
operazioni, 123
utilizzo dei messaggi accettati, 120
Posta bloccata
aggiunta all'elenco degli amici, 128
dove sono i messaggi bloccati, 125
icone nell'elenco messaggi bloccati, 122
invio di messaggi di errore, 134
modifica della modalità di elaborazione dei messaggi indesiderati, 126
operazioni, 123
ripristino di messaggi, 124
utilizzo dei messaggi bloccati, 120
procedura guidata di aggiornamento, 21
programmi potenzialmente indesiderati (PUP), 28

affidabilità, 32
avvisi, 31
eliminazione, 40
pulizia, 40
quarantena, 40
rilevamento, 39
rimozione, 31
programmi whitelist, 32
protezione da scrittura di un disco di ripristino, 43
protezione dei minori, 112

Q

Quarantena
aggiunta dei file sospetti, 40
eliminazione dei file, 40
eliminazione dei file sospetti, 41
gestione dei file sospetti, 40
invio dei file sospetti, 42
pulizia dei file, 40 to 41
ripristino dei file puliti, 40 to 41

R

Registro eventi
gestione, 70
informazioni, 61
visualizzazione, 71
registro eventi, 92
ripristino di messaggi, 124

S

Scansione
eliminazione di un virus o di un programma potenzialmente indesiderato, 40
opzione Analizza contenuto dei file compressi, 34
opzione Analizza sottocartelle, 34
opzione Analizza tutti i file, 34
opzione Ricerca nuovi virus sconosciuti, 35
opzione Ricerca programmi potenzialmente indesiderati, 35
pulizia di un virus o di un programma potenzialmente indesiderato, 40
quarantena di un virus o di un programma potenzialmente indesiderato, 40
scansione automatica, 37
scansione manuale, 33
scansione manuale tramite Esplora risorse, 36
scansione manuale tramite la barra degli strumenti di Microsoft Outlook, 37
verifica, 17 to 18
scansione
file compressi, 34
pianificazione delle scansioni automatiche, 37
programmi potenzialmente indesiderati (PUP), 28
script, 27
solo file di programma e documenti, 26
sottocartelle, 34
tramite Esplora risorse, 36
tramite la barra degli strumenti di Microsoft Outlook, 37
tutti i file, 26, 34
virus nuovi sconosciuti, 35
worm, 24
scheda di avvio rapido, iii
script
autorizzazione, 31
avvisi, 30
interruzione, 30
ScriptStopper, 27
segnalazione dei messaggi indesiderati a McAfee, 133
segnalazione di un evento, 67
Shredder, 94
SpamKiller
attivazione dei filtri, 101
disattivazione dei filtri, 101
pagina Posta accettata, 122
pagina Posta bloccata, 121
supporto tecnico, 40

T

traccia degli eventi, 66

U

utente di avvio, 83 to 84
utenti, 103
accesso a SpamKiller, 113

aggiunta di utenti, 110
cambio di utente, 113
creazione di password, 112
eliminazione di profili utente, 113
modifica dei profili utente, 113
tipi di utente, 111
utilità, 93
utilizzo di AntiPhishing Filter, 127
utilizzo di un disco di ripristino, 44

V

verifica di Personal Firewall, 54
verifica di VirusScan, 17
virus
autorizzazione per script sospetti, 31
avvisi, 29
eliminazione, 29, 39
eliminazione dei file infetti, 30
interruzione degli script sospetti, 30
interruzione dei potenziali worm, 31
pulizia, 29, 39
quarantena, 29, 39
quarantena dei file infetti, 30
rilevamento, 39
rilevamento con ActiveShield, 29
rimozione di PUP, 31
segnalazione automatica, 44, 46
VirusScan
aggiornamento automatico, 47
aggiornamento manuale, 47
pianificazione delle scansioni, 37
scansione tramite Esplora risorse, 36
scansione tramite la barra degli strumenti di Microsoft Outlook, 37
segnalazione automatica dei virus, 44, 46
verifica, 17
visualizzazione degli eventi nel Registro eventi, 64

W

whitelist
PUP, 32
Windows Firewall, 51
World Virus Map
segnalazione, 44
visualizzazione, 46
worm
avvisi, 29, 31
interruzione, 31
rilevamento, 29, 39
WormStopper, 24